Haaga-Helia
University of Applied Sciences Ltd.

The Awareness and Importance of Information Security amongst Young Travellers

Kaisu-Linnea Mäkelä

Bachelor's Thesis
Degree Programme in Hotel, Restaurant and Tourism Management 2015

Haaga-Helia
University of Applied Sciences Ltd.

Abstract

25.5.2015

Author
Kaisu Mäkelä

Degree programme
Hotel, Restaurant and Tourism Management

Thesis title	**Number of pages and appendix pages**
The Awareness and Importance of Information Security amongst Young Travellers	**48 + 10**

This research-based thesis looks into the knowledge of and behaviour related to information security amongst young travellers. The thesis process began in February 2015 and was completed in May 2015. The aim of the study was to discover the level of awareness of information security risks and current measures taken to protect data amongst travellers. The thesis was commissioned by F-Secure, an online security and privacy company, so the objective was to gather relevant and valid information the company could benefit from. Further, the intention was to discover the correlation between information security awareness and measures taken to protect data.

The theoretical part of this thesis consists two chapters. Characteristics that define the age group are presented in the first chapter along with the significance of the defined focus group to both the travel and technology industries. The following chapter includes an overview of information security and concepts within, specifically concerning mobile devices. Common threats and solutions are also described.

The empirical part starts with a discussion of the research methods chosen. The research was carried out by an online survey through an event created in Facebook. The sample group consisted of young travellers who own and carry a mobile device when travelling. The survey was open for a week and 210 responses were gathered. The online survey and analysis software Webropol was used to collect and analyse the data.

The results of the research supported the hypotheses of the study in that most respondents did not feel aware of information security risks and therefore did not use valid security measures to protect their data. The results suggest that in order to increase demand of information security products, awareness should be raised amongst the consumers.

Keywords
Information security, youth travel, mobile device, privacy, Generation Y

Table of contents

1 Introduction

The tourism industry is one of the steadiest growing industries in the world and youth travel counts up to over one fifth of international arrivals. In fact, the urge to travel can be seen as one of the defining characteristics of youth today, also known as Generation Y. Having been born into an emerging world of technology and growing up surrounded by laptops, smartphones and tablets, another essential aspect of Generation Y's life is being constantly plugged to technology (Gibson 2013). Information sharing is the primary purpose of online social networking and mobile devices are permitting the user to stay connected around the clock and around the world.

Furthermore, it is undeniable that most processes and services will move if not entirely but mostly to the online world. Tourism companies seek to keep up with the trends in technology and often try to get ahead of the game, all in attempts to make it as easy as possible for the customer to learn about and use their services.

The advantages of modern day technology and ease of communication has definitely made the every day lives of many a traveller easier but few have paid attention to the price that is paid. The countless free services that are offered to the consumer seem convenient but the truth is that they are paid for with information that is shared with the device, application, service, and so on. The question is would consumers be so willing to share all that information if they were aware of what they are giving up? Mikko Hyppönen (in Safe & Savvy 2015a) explains that what is nowadays defined as "smart", such as smartphone, smart TV up until smart toaster, can equally be considered exploitable. With the continuous feed of internet innovations grows the need for acts of security and privacy.

Furnell (2006) points out that it has been proven that the most significant contributors to security incidents are peoples' attitudes and lack of awareness of security issues. He continues by highlighting "the need to foster a culture in which users are aware of the security issues that pertain to them, and have the required knowledge and skills to act appropriately".

There are different ways to protect oneself from risks caused by the use of technology, which include both traditional solutions as well as solutions that are guided by your own actions regarding technical information security. These user-specific protection methods include common sense, reasonable use of internet and email, anti-malware software, system updates, auto-lock for devices, understanding and studying the issues and reporting any deviations. (Rousku 2014, 123-124)

1.1 The commissioning party

F-Secure is a Finnish online security and privacy company founded in 1988. The company employs over 1000 people in 25 offices around the globe with its headquarters in Helsinki. In 2013 revenue reached 155 million euros.

F-Secure has grown to be a world leader in security and has held on to its values: privacy, integrity, transparency and trustworthiness. F-Secures primary mission is to fight for digital freedom with the company slogan currently encouraging to 'Switch on Freedom'.

> In the digital world, it seems like everyone wants a piece of you – hackers, Internet trackers, online spies. We believe you should have the freedom to live your digital life without worry. It's our passion for freedom that pushes us to create better products and services to enable and empower you. For us, freedom is about making sure you are the one in control of your digital life. Together with you, we're fighting for your digital freedom. (F-Secure 2015c)

According to F-Secure, there are three crucial elements to be addressed to achieve digital freedom: security, privacy and identity. One of the fundamental human needs is **security** and safeguarding what is valued. **Privacy** includes the right to be able to choose what is made public and what remains private, and control of ones own **identity** is everyone's indisputable right. As illustrated in image 1, each sphere embodies a range of issues and concerns, which can overlap and interchange in various ways. Furthermore, each person has their own view and special balance of security, privacy and identity. F-Secure aims to provide tools and services for the consumer to be able to gain control of these elements themselves. (F-Secure 2015c)

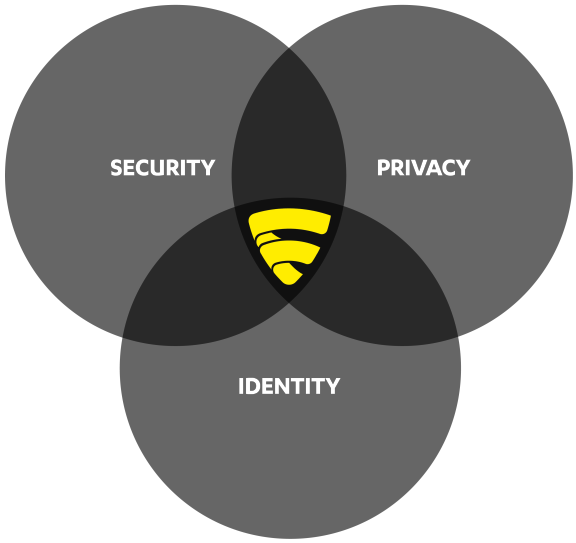


Image 1. Security, privacy and identity (F-Secure 2015c)

Besides the traditional anti-malware software and firewall products, these services and tools include various reports, guides, news and blogs that provide the consumer with in-

formation concerning online security and privacy, and current issues and threats in the online and mobile landscape.

F-Secures most relevant products in the market at the moment are:

- F-Secure Safe - provides protection for all devices and online threats.
- F-Secure Freedome - a private VPN, which allows the user to use any public WiFi or Hotspot safely and privately, access favorite internet services when abroad and prevent ads and sites from tracking.
- F-Secure Key - allows the user to store all passwords and credentials securely and provides news feed for hacking alerts.
- F-Secure Mobile Security - for mobile devices specifically, protects against harmful apps, viruses and other malware.
- F-Secure App Permissions – tracks which apps may threaten privacy and filters apps based on the permissions they require.

(F-Secure 2015c)

1.2 Research problem, background and objectives

The author of this thesis started working for the commissioning party in January 2014. After joining F-Secure, she realized that news on internet and online security, or namely, its breaches, was everywhere. She also noticed that the company itself and its experts were highly appreciated in the field. The author soon understood that the potential for the company's growth was immense as long as it got its message through.

It was when the author found out that the innovation team in the company was planning to develop a product targeted for travellers and was asked to join the project that she got the idea for the topic of this thesis. One main question remained throughout the development and marketing concerns of the project: are travellers aware of the risks of data vulnerability and what are their current actions in safeguarding sensitive and personal information?

This question essentially formed the **aim** of the thesis, which is to find out the level of awareness and current processes of information security amongst young travellers. In order to accomplish this, two **objectives** for the research were formed:

1. To gather informative and trustworthy results that can benefit the commissioning party.
2. To discover how the level of awareness of information security risks affects the online privacy behaviour of young travellers.

According to the first objective, two **hypotheses** for the research were established:

Hypothesis A: The young traveller lacks knowledge of current information security risks.

Hypothesis B: The young traveller is not securing his or her data.

However, the second objective is to find the correlation between these two hypotheses so the correlational hypothesis is in form:

Hypothesis C: The level of awareness of current information security risks of the young traveller affects whether he/she protects his/her data.

1.3 Purpose and scope

Since June 2013, after major revelations of NSA surveillance issues made by Edward Snowden, internet security has become a hot topic in the world today. Consumers have become conscious of what information they are sharing on the web and concerned about their online privacy. This has opened up the opportunity for internet security companies to step forward and gain new markets, which is exactly what the case company of this thesis has been doing ever since. F-Secure, recognized for its 26 years of expertise and awarded internet security software, has since then began an era of transformation, making the business more aggressive by renewing strategies, broadening their product lines and targeting new market groups.

The purpose of the thesis is twofold. Information is gathered and studied to provide a more detailed overview of the young traveller as a potential target market to the commissioning party. Their behaviour is researched to establish the current level of demand for online security services. On the other hand, relevant and current information about information security issues and privacy threats are presented to the young traveller and awareness is raised amongst them.

The scope of this thesis limits the depth of the vast topic of information security. As the author is a student of hospitality management, it is of most relevance to research only the most essential and critical issues of information security, and specifically concerning the traveller. This includes mainly threats against mobile devices and risks that are augmented when leaving the home country, merely scratching the surface of the ever more diversified realms of online security. In addition, the scope of an applied sciences bachelor's thesis usually does not permit reaching large enough sample groups that could be generalizable to the whole population, in this case young travellers all around the world.

1.4 Structure of the study

After the introduction, which includes a short description of the main concepts covered in the thesis, the presentation of the commissioning party, a description of the aims and ob-

jectives of the study and finally a discussion on the purpose and scope, follows the theoretical part in two main chapters. They cover the main concepts in more depth, which are youth travel and information security.

The first of the two chapters begins by defining the specific age group that is referred to as 'youth' and its subchapters reveal the significance of the demographic group to both the tourism industry as well as the technology industry; two of the fastest growing industries today. Chapter 3 will then present information security, the concept of privacy, current day threats and provide solutions while on the road.

The theoretical framework is followed by the empirical part, also in two chapters. Chapter 4 outlines the research methods, giving a more detailed description of the research approach and sample, survey, and data collection methods and analysis. A quantitative research method via online questionnaire carried out in the social media was chosen to answer the research statements of the study. At this point, the validity and reliability of the study is assessed. Chapter 5 describes the data gathered and presents the findings and analysis of results. Finally, the discussion part will offer an overview and conclusions of the study as well as directions for further research. The thesis process will also be assessed along with comments from the commissioning party.

2 The young traveller

In this chapter the target focus group is introduced. The purpose is not only to validate the significance of this specific market group but to also create a general image of the potential of the market to the commissioning party.

Firstly, the definition of 'young' in this thesis is specified from various aspects. The first subchapter presents the significance of tourism to the global economy in facts and recent figures to establish the role of youth travel in tourism. This is followed by a second subchapter considering young travellers as mobile device users.

There are various definitions for today's youth. In terms of generations, Generation Y, also known as the Millenials, can be considered as youth today. While there is no definitive age range for this generation, many suggestions have been made to categorize the Millenials or Gen Y. According to Wallop (2014) and Tchacos (2012), they are born between about 1980 and 2000, making them 15-35-year-olds in 2015. In a research from Forrester (in eMarketer 2013) concerning smartphone and mobile adoption, Gen Y was defined as consumers between the ages of 24 to 32.

In terms of youth travel, youth travel consultancy Student Marketing (2015) defines Youth Travel as independent trips made by 15-30-year-olds, and lasting less than a year. The range has recently expanded from 18-24 to 15-30 years old and beyond, due to demographic changes in western societies such as longer study time frames and older age for marriage (WYSE Travel Confederation 2014a). More and more members of Generation Y are putting off marriage, mortgages and desk jobs and choosing to see the world instead (Tchacos 2012).

Beside the age label, Generation Y has also become a symbol of a new 'culture' entailing a unique set of values, skills and behaviours that surpass geography and ethnicity. Academic literature has only recently begun to consider the consequences of this emerging culture as they enter the workforce and start to have larger amounts of disposable income. (Yeoman, Hsu, Smith & Watson 2001, 89)

2.1 Tourism and youth travel

In the most recent publication of the World Tourism Barometer from UNWTO, international tourist arrivals in 2014 increased by 4,4% reaching 1,135 million, compared to the 1,087 million arrivals in 2013. The report indicates an average 5% annual growth in international tourist arrivals since 2009. (UNWTO 2015a, 1)

The continued growth and deepened diversification implies that tourism has become one of the fastest growing economic sectors in the world. Image 2 illustrates the social and economic phenomenon that is tourism, showing its significance to the global economy in figures. It shows that tourism amounts up to 9% of GDP, generates 1 out of every 11 jobs and represents 6% and 30% of the world's exports and services exports respectively. (UNTWO 2015b)

Image 2. Tourism figures as part of the global economy (UNTWO 2015b)

Rifai (in UNWTO 2015a, 1) points out that spending on international tourism has showed significant growth in 2014, which proves the tourism sectors capacity to stimulate economic growth, boost exports and create jobs, even in a scenario with decreasing commodity prices. He refers to the export earnings from international tourism and passenger transport reaching 1.5 trillion US dollars in 2014.

Chapman (in WYSETC 2014b) noted that the amount of international trips that young people take is increasing consistently and travel is becoming an established part of their lifestyle. Herrschner (in Tchacos 2012) describes Generation Y as a very independent and individualistic generation, which makes travelling a natural course in life. In fact, young people accounted for over 20% of the 940 million international tourists in 2010 (UNTWO in WYSETC 2014a) and are predicted to reach 300 million by 2020, representing a 59% growth in 10 years (WYSETC 2014a). Youth, student and educational travel is a continuously growing industry, despite the global economic downturn, and is one of the fastest growing markets within the tourism industry (Student Marketing 2015; WYSETC 2014a).

2.2 The young traveller and the use of mobile devices

Herrschner (in Tchacos 2012) says that Gen Y is the first digital generation. The internet is driving the tendency to spend long periods abroad as it makes it possible to continue taking part in social life at home. As Generation Y was born somewhere between the in-

troduction of the Walkman and the founding of Google, it is not a surprise that they are shaped by technology (Wallop 2014).

The research firm Forrester (in eMarketer 2013) found that Gen Y led the US in smartphone and mobile adoption showing that 72% of consumers owned a smartphone. According to WYSETC (2014a) up to 79% of the youth segment own a smartphone, which makes it the segment with the highest penetration of smartphones globally. Similarly, a survey requested by the European Commission (European Union 2015) confirmed that the use of a mobile device for accessing the internet is significantly higher among young people aged 15-24 compared to 55-year-olds and over. Concerning smartphones the usage was 85% among the younger age group and 30% for those aged 55 and over.

The reason for their domination in the market was supported by the fact that members of Gen Y are young enough to appreciate smartphones and still old enough to afford them, whereas younger consumers don't have the money and older consumers don't value them as much. It is suggested that Gen Y will be smartphone power users for many more years to come. (eMarketer 2013)

Furthermore, a separate study confirmed that the age group was most likely to use mobile and tablet applications (eMarketer 2013). Applications are becoming more and more important in the tourism sector to both companies providing the service as well as for the travellers using them. There are applications that provide assistance for every stage of the trip (Tourism Business Portal 2010, 2), which, according to Clack (2015), can be divided into

- planning
- booking (Skyscanner, Hostelworld, etc.)
- navigation (e.g. Waze)
- exploring (e.g. TripAdvisor)
- communication (e.g. Whatsapp)
- documentation (e.g. Instagram).

Manglis (2010) further identifies the main applications of mobile services in tourism as localisation, routing, location of points of interest (augmented reality), information about travelling conditions, reservations, travel schedule information and suggestions (advertising). The main benefits of the diversified market of tourism related apps are smoother and faster reservation processes, lower costs, access to local information and ability to share experiences (Tourism Business Portal 2010, 9).

Hannam and Diekmann (in van Vaals 2013, 15) define the ten most popular during-trip technology related activities or statements amongst 25-34-year-old travellers in order of popularity:

- Using email as means of staying in contact with family and friends.
- Preferring hostels providing free internet or WiFi access.
- Adding people met during the trip to social networks.
- Booking future travel online.
- Keeping a journal.
- Using social networks as means of staying in contact with family and friends.
- Changing travel plans after finding information online.
- Using call cards or call centres or send postcards or letters to keep in contact with family and friends.
- Using online traveller related forums for information for further plans.
- Posting pictures online while travelling.

Similarly, an infographic produced from a research by Insites Consulting (in Van den Bergh 2013) suggests that over 8 of 10 internet users amongst Gen Y are members of a social network and 80% log on daily. It also listed the top drivers to use social media, which included communicating/sending direct messages, killing time, sharing photos and sharing information and links. It was established that of all online social networks, Facebook is the most known network with 91% awareness along with highest membership rates with 66% of all respondents being a member compared to the second highest, Twitter, with 29%.

Dickinson, Ghali, Cherrett, Speed, Davies and Norgate (2014, 15) suggest that there is potential for even further collaboration of social assistance in the tourism domain due to the growing importance of social networking and potential for wider social assistance in travel. In order to develop trusting communities and providing travel assistance, a certain degree of personal information exchange is required.

However, privacy and security issues arise with the transmission of individuals' data by apps to unknown providers with little or no user knowledge of this taking place. This can be rather distressing especially as this data might include sensitive data, such as records of user location. Another issue is the growing tendency of uploading personal information to shared communities, raising concern about abuse of trust and significant security issues. This causes pressure for the developers to work on continuous analysis and creating rigorous systems to maintain a necessary level of privacy in order to provide safe and secure systems for users. (Dickinson & al 2014, 15) Ultimately though, it is in the hands of the users themselves whether their data remains private, which brings us to the next chapter regarding information security.

3 Information security

This chapter introduces information security as a current topic not only in the technology industry, but also for companies and consumers alike. Consequently, both the concept of privacy and the identification of the type of information users have and would prefer to keep private will be detailed. This is followed by a discussion of the threats that are posed against our fight for privacy in the mobile era, and completed by solutions that consumers can and should implement in their daily actions. Finally, there will be a summary of the main concepts that have been covered in the theory part of this research, in order to illustrate the common relevance of the topics.

First of all, it is important to establish what information security is. Information security essentially attempts to reach three goals, the first of which is to keep information **trustworthy** and within the reach of only the right people. Secondly, information needs to stay **whole**, so that only authorized modifications may occur. Finally, information should always be **available**, devices usable and services must work when they are needed. (Järvinen 2012, 10)

Mobile security refers to the information security of smartphones and tablets, the most relevant accessories of travellers. An important and most used feature of these devices is apps, or mobile applications. Apps are software that are specifically made for mobile devices and improve delivery of services in the mobile environment. Since nearly anyone is able to develop apps, it has led to a revolutionary opportunity to exploit the mobile computing capabilities of smartphones. (Dickinson & al 2014, 3) Concerning mobile technology, there seems to be a fine line between staying on top and keeping security issues under control (Crossland 2014c).

To validate the necessity of information security, it should be reasoned why it is so important. The smartphone contains the owners personal life in a miniature version: emails, call records, location, friends and family contact information, messages, calendar and even passwords for different applications. No other device is as important in everyday life. (Järvinen 2012, 30)

That said, smartphones and tablets are the most difficult environment when it comes to information security. They are easy to lose and steal, the devices don't last the everyday use and the security features can't quite keep up, resulting in various technical security gaps. This can partly be explained by the fact that mobile devices have multiple parties involved: the manufacturer, platform, application, cloud service, operator and so on, and the user has no way to make sure that each party is secure or legitimate. (Järvinen 2012,

52) More to the point, it is not uncommon to become a victim of data loss nowadays. News on data loss can be found daily in the headlines worldwide. Despite many devices having regular security precautions such as passwords, there is still a fair amount of concern about how the information can be used and what it can result to. (Pound 2009)

The smartphone is undeniably a useful and versatile travel companion. The less you need to carry with you, the nicer it is to travel. The smartphone fits into your pocket and replaces many different devices: the camera, navigator, radio and MP3 player. (Järvinen 2012, 272) It also allows you to stay in contact with family and friends at home, connect with new acquaintances and look for reliable information in social communities for travel tips. The disadvantages of these useful aspects of mobile technology are the threats that become more pronounced once on the road (Safe & Savvy 2015b). Therefore, when travelling abroad, it is exceptionally justified to be alert and make sure that personal data is secured (Tranberg & Heuer 2013, 81).

3.1 Privacy – What exactly it is we should hide

While it seems that users are getting a wide range of products and services in form of apps on their devices for free, the truth is that they are paying with their privacy. They give away information, and the value of such data has recently become a kind of digital currency (F-Secure 2015b).

The Latin root for the word privacy is based in the thought that a part of our lives is separate, *privatus,* in relation to the state, officials or the public. Nowadays, privacy has been given a whole new definition. Privacy today is a person's own ability to decide for themselves who knows what about them, where and in which context. (Tranberg & Heuer 2013, 15) Privacy is most often taken for granted as its meaning and worth is not recognized before it is lost. Especially in Europe it is commonly assumed that the law will protect anyone from privacy violations but ultimately, the reformed definition of privacy contradicts the notion. (Tranberg & Heuer 2013, 21)

Companies seem to be collecting, consolidating, analysing and selling user information while withholding it from those it was initially collected from. Consumers, however, are starting to acknowledge how much of their personal information is available to these companies and how their personal preferences are considered 'fair game'. (McMullen 2014) Snowden's leaks have escalated this awareness to a whole new level and it has become common knowledge that governments and corporates are keeping an eye on people (Safe & Savvy 2013). Still, Soghoian (in Tranberg & Heuer 2013, 47) expresses that the average consumer does not have a clue of the extent of what tracking online can do and

criticizes advertisers for doing their best to keep the consumer out of the loop. He suggests that the whole internet business is based on the ignorance of the consumer.

A common argument in talks of privacy and security is “I have nothing to hide” (Safe & Savvy 2013) but this is generally a fallacy. In most cases, people are not even aware of what pictures, documents or information are saved on their devices, or cannot possibly recall each and every file. There will inevitably be a few that would preferably be kept to oneself if it came to it. Moreover, there may be something concerning someone else, such as information or photos of a friend or family member. It is impossible to be entirely sure that there is no information that could be harmful to them, now or in the future.

Tranberg & Heuer (2013, 23) suggest that in the digital world, the expression ‘personal identity’ would be a more appropriate term for privacy or private life when taking into account the challenges of today. A user’s identity is constantly under siege, without them ever noticing. Indeed, another recurring argument is “I’m a nobody, what are they going to do with my information?” While Tranberg & Heuer (2013, 24) do point out that the value of a certain person’s identity depends on who they are and though this might be the case today, it is impossible to know what one might become in the future. Information that is once online will be online forever and can be scooped up at any moment by officials, a future employer, insurance company or bank.

Sullivan (in Safe & Savvy 2015c) suggests that it may simply be a matter of posing the right question to help the consumer fully comprehend the value and term of privacy. In a survey made by F-Secure in the United Kingdom, 83% of respondents who were asked the question “do you have something to hide?” answered “no”. When the question was turned the other way around in form “would you want to share everything about your life with everyone everywhere, all the time, forever?” up to 89% of respondents said no. (Safe & Savvy 2015c)

The first steps in protecting privacy are to know what’s at play and consider the value of the information concerning the user and the identity built of them (Tranberg & Heuer 2013, 38). This can be determined by considering the information saved on a smartphone, tablet or laptop concerning home, private life, work, money, free time or any other matters that the owner would not want to end up being *lost, modified or public* (Rousku 2014, 124). It can even be virtual property that the user is not even conscious of having and may have significant financial impact. Some examples are licences, such as Windows, Office and games, downloaded songs, books and movies, and even strengths and features the user might have gained through games. (Rousku 2014, 146-147) Other more obvious examples of data users might want to protect are pictures, documents, access to emails, work

email, user names and passwords, and contacts. Most people even keep something as common and simple as a CV on their devices, which most often contains sensitive information such as ID, address, phone number, etc.

Nevertheless, there are people who think that the advantages of digital services, such as keeping contact with family and friends, saving time and money, and so on, are so weighty, that privacy is not worth worrying about; they consider privacy already dead and forgotten (Tranberg & Heuer 2013, 15). Järvinen (2012, 24) explains this by stating that user comfort and security are in conflict. People believe that things can either be made secure or easy to use but never both at the same time. Furthermore, even if the user knew everything there is to know about information security, they would still ultimately choose comfort over security; they want the programs to work fast and be able to choose the devices and applications they want whenever and wherever they wish. The reason for this, however, is very simple: security threats are invisible and abstract whereas usability factors are concrete and current.

Further conflict occurs as Generation Y can be characterized as being comfortable sharing their life online (Wallop 2014). Very few actually consider what damage such limitless sharing of information and default openness can cause to their identities and positions as family members, students and teachers, employers and employees, consumers and citizens. (Tranberg & Heuer 2013, 13)

While it is expected that a reformation in data collection practices might take place in the near future, it is in the consumer's best interest to take care of their own data privacy and understand how much of it is currently being collected and used. (Crossland 2014a)

3.2 Threats – Who, how, what and where

According to Drevin, Kruger, and Steyn (2006), there is a vast range of threats to information security that include human errors, theft, technical errors and acts of sabotage.

It should be noted that while the internet is worldwide, the laws and authorities are national, which makes it very easy for criminals to turn to the internet to look for their next victims. Internet criminals steal credit card information, personal identification and user names and passwords, which are easy to turn into cash. (Järvinen 2012, 22) In fact, Hyppönen (2015 in Safe & Savvy 2015a) points out that online crime is the most profitable business in the IT industry.

Mortleman (2009) suggests that some of the most common data security hazards for business travel, which forms a big part of youth travel, are loss or theft of equipment, data

theft through WiFi, spyware on PCs in airports and hotels, and customs or border officials in countries prone to corruption. He continues by stating that airports worldwide are renowned centrals for theft and pick pocketing. A recent survey suggests that London Heathrow airport is the biggest offender for lost and stolen devices with close to 900 devices going missing per week (Blevins 2014). Furthermore, modern IT infrastructures are able to acknowledge and measure each passer-by in their vicinity, an example being the information chips in new passports that are read just by passing through the checkpoint (Tranberg & Heuer 2013, 23).

Cluley (in Mortleman 2009) explains that real risk in **data vulnerability** is obviously not the cost of replacing the device but the value of access to the information for cybercriminals. The danger is that they will be able to access confidential, sensitive information that can be exploited by identity thieves, along with usernames and passwords, that could even lead to corporate espionage in the case of business travel.

It is not even necessary for any device or hardware to leave the owners possession for the data to become compromised. Network connections in public internet cafes, airports or hotels can usually cause the same damage to a device. (Mortleman 2009) It is needless to say that most travellers, especially those of Gen Y, will wish to access the internet even when abroad and try to avoid expensive roaming costs. Without the feeling of seemingly secure mobile networks provided by their operators, travellers are forced to turn to **public WiFis**.

Wireless Internet is known as WiFi, Wireless Fidelity, which refers to the mutual compatibility between devices. It is very comfortable as it allows free mobility. (Järvinen 2012, 274) However, WiFi in general was never designed to be particularly safe, causing it to expose sensitive information to the public (Safe & Savvy 2015b). In fact, all users connected to a certain network are able to see one another's traffic with just a few simple moves. Some may have an analyzer program, which picks out interesting IP packages and snatches e.g. passwords, usernames and credit card numbers of the other users. The risk is greatest in public networks where there can be simultaneously hundreds of users. (Järvinen 2012, 275)

In many public areas, such as airports and hotels, it is extremely easy for someone to set up a fake WiFi network, name it 'Public' or 'Secure' this or that, and attract people to connect to it with the intension of gathering the personal and sensitive information of any user (Cluley in Mortleman 2009). No matter how trustworthy the name of a public WiFi appears, it is hard to know who actually administers the network. They can follow and monitor all information traffic that is not protected. Cluley (2009, in Mortleman 2009) reveals

that a business centre in a hotel can, in many cases, be less securely managed than a popular cyber café. Considering small hostels where young travellers tend to stay, it is hard to expect them to have any knowledge or ability to secure the WiFi they provide.

The threat of **hacking into accounts**, which can be a consequence of using public WiFi unprotected, can result in more than just data loss. Cyber criminals may use email accounts to send spam or scam, or even targeted attacks. Another danger is the loss of reputation. The criminal can use social media accounts not only to collect further information of the contacts, but also to publish any information they desire under the users name. (Rousku 2014, 149)

Another significant threat is the **misuse of a device** i.e. when cyber criminals use one's device against them, their work place or other organizations (Rousku 2014, 124). This might include using the device as a spam or scam server, malware downloading server, warez site (illegal commercial software distribution server), or child porn distribution server (Rousku 2014, 146). **Misuse of personal data** on the other hand can be considered as the unconsented use of personal information for, for example, marketing and sales targeting.

In addition, each year, millions of **identity thefts** happen around the world. Sometimes it might be part of large scale hacking where millions of customers are exposed, such as the attack against the Sony entertainment network in November 2014, or attacks against certain credit card companies. Other times it can be a spiteful attack against an individual. The problem is so common that, for example, Canada has founded a national help center where identity theft victims can go for help. (Tranberg & Heuer 96, 2013) Furthermore, in most cases, the carrier of the device does not even know they're being robbed because digital information does not disappear; it is merely copied without consent and, often illegally, used for further use. (Tranberg & Heuer 2013, 24)

With regard to **mobile applications**, a research by Ponemon Institute (in Tamarov 2015) revealed that only 6% of money spent on mobile app development is allocated to security purposes. They also discovered that half of the companies didn't devote any budget for security and 40% weren't scanning their apps for vulnerabilities. Furthermore, another research (in Tranberg & Heuer 2013, 79-80) showed that free applications were four times more likely to locate the user, three times more likely to get hold of their contacts and two and a half times more likely to get their hands on their camera and photos, compared to paid applications.

Mortleman (2009) emphasizes the increased risk of devices and data being stolen, inspected or impounded when travelling. He continues by highlighting the importance of awareness of the augmented danger and measures to be taken in the event of any issues that may arise. Furthermore, these should be combined with strict procedures for data transportation, access and storage and supported by qualified technologies.

3.3 Solutions to keeping personal information personal

According to various studies, many people are concerned about their privacy, but the question is, do they act on it? While many people worry about Google's various "free products", very few have stopped using Google completely. Even fewer read the terms and conditions texts, which they agree to when taking a new service to use. (Tranberg & Heuer 2013, 30)

Legislators around the world are feverishly discussing how citizens and consumers could and should be protected. However well the authorities and legislators succeed in protecting us, laws and regulations are always behind in terms of what happens in the real world. This means that each individual must monitor their own interests while it is still possible and before technological developments make it too hard to fix things. (Tranberg & Heuer 2013, 14-15)

Three simple and most essential practices suggested by Sullivan (Safe & Savvy 2015b) are to lock the device with a PIN number or passcode, remove files that are not needed during the trip, and test VPN connectivity.

To start with the basics, it is recommended to keep devices within reach and sight at all times, especially in busy and crowded places, and to protect devices with PIN codes and other auto-lock mechanisms (Emory University 2015; Rousku 2014, 158). A relatively worn out topic is the use of complex and unique passwords for all accounts that should also be changed from time to time. The reason for the continuous emphasis on passwords is that the foundation of information security of services is based on them, and they also function as insurance. (Rousku 2014, 159)

Lackey (2014, in Blevins 2014) advises travellers to carry as few devices as possible with them, especially as in some cases it is even illegal to bring types of software or hardware to certain countries (Emory University 2015). In addition, all software should be updated to the latest version available. Criminals are continuously searching for ways to hack into devices and a single software that is not up-to-date is enough to do so.

To further enhance the security of data, Lackey (2014, in Blevins 2014) suggests backing up and removing irrelevant data and applications before leaving and reinstalling them only upon return, though recognising the improbability of most users taking such drastic security measures. Emory University (2015) regulations however state this as the number one safety precaution. Devices continuously store information regarding the users actions, internet browsers store a history and apps create temporary files. Furthermore, many apps and websites store passwords and contact information that can be compromised while travelling. (Sullivan in Safe & Savvy 2015b)

Backing up data will help getting it back in case the device gets stolen. It is most important with sensitive and confidential information, which should essentially be removed from the device completely. The best option is to travel with only the data needed during the trip. In cases where some sensitive data needs to be stored during travel, encryption is paramount in order to prevent criminals in gaining access to the data if stolen.

Concerning the actual travel documents, which obviously hold valuable sensitive data, Järvinen (2012, 277) suggests the following:

- Scanning of passport and other possible travel documents in jpg format.
- Saving pictures on a USB stick or memory card.
- In ticketless travelling, documents and confirmations are mostly emails, so it is important to save them as documents and print a paper copy to take along just in case.
- The e-ticket via email or app does not necessarily need internet as it is possible to take a screenshot of the ticket and present that at the control.
- Carrying a charger along.

When accessing the internet abroad, it is best to be sceptic about open wireless networks. The safest way to browse the internet anonymously on public networks is to use a VPN - Virtual Private Network. The VPN hides the users IP address or creates a new address for each login. Further benefits of using a VPN are getting neutral offers online that are not based on web history or IP address and accessing services that are only available from a certain country. (Trannberg & Heuer 2012, 243) According to Sullivan (in Safe & Savvy 2015b) almost every security researcher swears by them, especially while travelling because the user is more exposed when away from home. Additionally, it is critical to remember to disable automatic connection to WiFi spots, and assume that anything done over public WiFi is part of a public conversation (Safe & Savvy 2014).

It is also advised to enable firewalls and install antimalware software, which are still considered the foundation of computer software (Rousku 2014, 158). They will help protect devices while connected to unknown unsecure networks (Emory University 2015).

After returning from the trip, any passwords that were entered on public computers should be changed (Emory University 2015) and the WiFi access points used deleted (Safe&Savvy 2014). It is also a good idea to run a virus and spyware scan on the devices.

Tranberg and Heuer (2012, 228-229) made an interesting point regarding sharing holiday plans on social media networks and posting photos during the trip: they compared it to publicly welcoming criminals to break into their homes and informing that the house is empty. The gist is that insurance may not cover the damage if it comes to their knowledge that it was publicly announced on the web.

The solution is not to stop using the internet, mobile or social media, they are far too useful to throw away (Tranberg & Heuer 2013, 14), but to be aware of the threats and to ensure proper protection. As smartphone users, people are being followed at all times. Companies copy and download contacts and photo album type information without letting the users know. Because this kind of data is almost impossible to delete, it is indispensible to think hard about security settings and actions already before downloading and installing applications. (Tranberg & Heuer 2013, 74)

3.4 Summary of theoretical framework

The youth travel sector is a market of leading technological innovations and a learning ground for the whole travel industry due to the fact that young travellers are early adopters of every new technology (WYSETC 2014a). This essentially argues for the selection of the target focus group as the sample for research on information security behaviour.

Figure 1 illustrates the connection between the concepts discussed in the theoretical framework. The topics examined in the first chapter and the overlapping of terms form the concern and reasoning for researching information security.

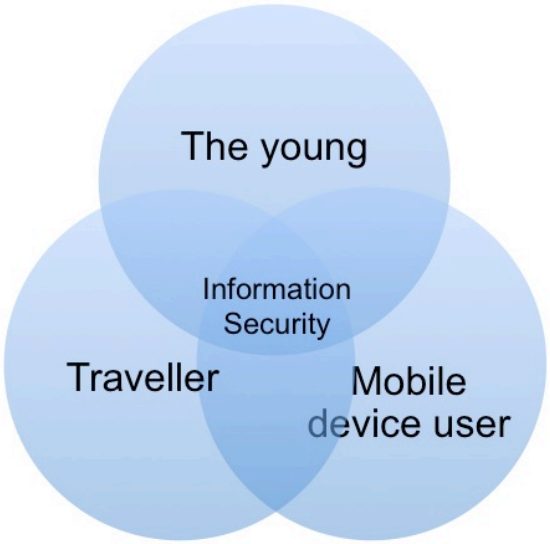


Figure 1. Summary of theoretical framework

Essentially, information security is the protection of *confidentiality, integrity and availability* of data stored on devices. The theory of information security presented the two main types of data in need of protection: privacy and identity. Common threats that were considered were those of data vulnerability, public WiFis, hacking, misuse of device, misuse of data, identity theft and mobile applications. Solutions or actions against these threats were introduced as listed below:

- PIN codes and auto-locking.
- Secure and safe passwords that are changed at regular intervals.
- Carrying along only relevant devices and data when travelling.
- Confirming that all software is up-to-date.
- Backing up, removing or encrypting vulnerable data.
- Use of VPN, firewalls and antimalware software.
- Avoiding public computers and WiFis without protection.
- Considering what is posted on social networks.

4 Research methods discussion

This is the first part of the empirical part of the thesis. In this chapter, the research strategy will be described and methods discussed. The chosen method was a mixed methods research carried out by an online survey. The research sample consisted of young travellers aged 18-32 and the survey was distributed through the social network Facebook. The survey tool Webropol was used to collect and analyse the data, and used to later transfer the data to Excel. The reliability and validity of the study is already considered at this stage and will be discussed throughout the methods selection process.

In order to be able to reason the research methods and base the findings, it is worth looking at the research problem as a whole together with the research objectives and formed hypotheses. Figure 2 illustrates the research problem.

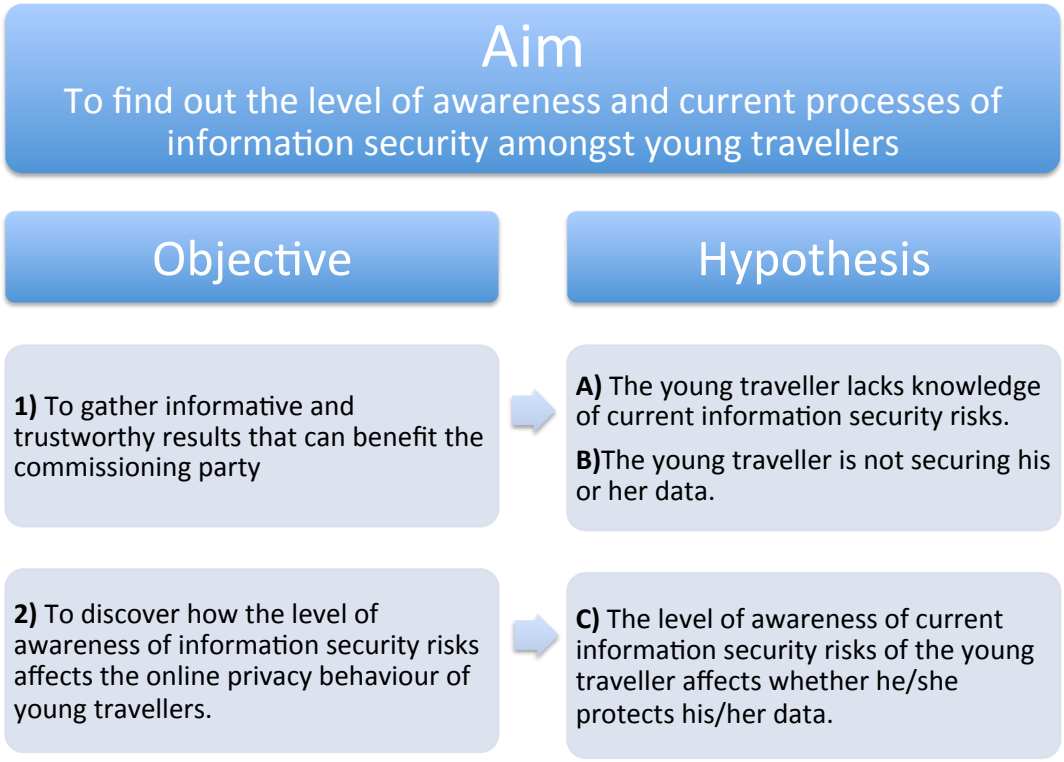


Figure 2. Summary of research problem

This summary will guide through the research methods discussion. Objective 1 suggests that the data and results collected through the study should be generalizable, so that they can be used in considering how to approach the new target group. Hypotheses A and B determine whether there is demand for security products. Objective 2 on the other hand

will explain whether the awareness of the importance and necessity of information security have a relation on measures already taken, which is what hypothesis C aims to prove.

4.1 Research approach

There are generally two different kinds of research approaches: quantitative and qualitative. The main difference between the two is that quantitative research aims to answer questions what, where, how much and how often whereas qualitative research defines why, how, and what kind? Furthermore, the quantitative approach sample tends to be numerous and representative. The qualitative on the other hand involves a narrow and discretionally assembled sample. It is however possible to use both approaches to complement one another. (Heikkilä 2008, 16-17)

The chosen approach was mostly quantitative due to the objectives of the research though some qualitative data was also collected. The quantitative approach seeks to collect facts and study the relationship of one set of facts to another and use techniques that should be able to produce quantified and possibly generalizable conclusions (Bell & Waters 2014, 9). A well-established method for capturing opinions, attitudes or to gain insight into the behavior of a certain population is surveys or questionnaires (Franklin 2012, 171). Different types of approaches to conducting surveys include phone, face-to-face and online. The selected method was an online self-administered survey via social network in order to reach the widest possible audience.

The advantages of online surveys are considered as being inexpensive to administer, being environmentally friendly and the ability to collect data very quickly. In addition, the augmented amount of smartphone and tablet users increase the possibilities of reaching a wider audience over the internet. (Andres 2012, 50-51) Furthermore, as it has been established already in the theoretical framework, members of Generation Y and the research sample own the most mobile devices and are generally members of at least one social network out of which Facebook is the most common.

The self-administered survey format implies that the respondent completes the survey with no help or guidance of an interviewer. This means that they are able to complete the survey at a time most suitable for them and as a result, responses may be more reflective and honest. However, this is assuming that all the components of the survey are clear, straightforward and unambiguous. (Andres 2012, 47)

The survey was conducted using the online survey and analysis software Webropol, which allows the researcher to collect data and minimize the risks of error in data saving.

This ensures that the data is reliable as it collects and saves the data automatically and it is easily transferred to Excel format.

4.2 Constructing the survey

Once the research plan, conceptual framework and research problem were clear, the planning of the survey began. Andres (2012, 117) suggests that the content of the survey items should be clearly defined based on proper background research for them to be valid. All research questions were formed keeping the findings from the theoretical framework in mind. The survey and all related materials were produced and published in English, as it is the most common language amongst travellers and a prerequisite for international travel.

Considering the research participants, it was important to keep the survey quick, clear and simple to attract as many responses as possible. Also, different kinds of survey questions ranging from closed dichotomous questions to open-ended questions were used, in order to keep the respondents interest and focus. In terms of analysing and answering the research problem, only the relevant questions were asked and the survey questions and options were kept strictly limited. The survey consisted of 10 questions in total, divided into 7 sections (Appendix 1).

The first three questions of the survey were to determine the demographic factors of the respondents. Questions regarding age, nationality and gender were asked. The age was selected from a pull down menu, and limited the respondent within the age range of 18 to 32. Although the widest range considered as youth travellers and Generation Y presented in the theoretical part was considered 15-35-year-olds, the age range was modified due to ethical considerations and issues affecting the analysis of the results. The minimum age 18 was set as according to ethics, minors require consent in order to be able to respond to a research survey. Furthermore, it was predicted that 25 would be the average age of respondents, as most of the participants within the research sample were of the same age as the researcher. This way, 25 would be the median of 18-32.

Options for nationality were Finnish and other, and the respondents were asked to specify which if the option ‘other’ was selected. Again, it was expected that most respondents would be Finnish but it would be interesting to find out the responses of people from different nationalities and how they varied.

Questions 4 and 5 consequently focused on the travel habits of the respondents concerning travel frequency and the mobile devices they carry along when travelling. The question regarding travel frequency was specified as referring to trips abroad due to the importance

of an augmented use of public WiFis in order to avoid roaming costs. Threats caused by using open, unidentified networks are an essential topic in the theoretical section. The respondents had the possibility to answer '0' to trips made annually, so that the research sample could be better controlled. It would be easier to later extract these respondents from the results if necessary, as they would not be relevant for the study. Similarly, the option 'none' was provided for the devices applied for question 5. For the other options, only the relevant mobile devices for the study were provided.

The rest of the questions were considered as individual themes. Question 6 was set to determine the kind of information travellers keep in their mobile devices when traveling and points of risk. No further options or open answers were provided as the goal was to determine the nature of information respondents maintain on their devices and which online risks occurred to their use of internet.

This was followed by a question regarding information security awareness. It was presented in rating scale. One of the suggestions prior to the release of the survey was making this an open-ended question. While agreeing it would certainly be interesting to find out what it was that people considered they knew about information security, I feared scaring away the respondents. One of the reviewers of the survey commented that they would feel "quizzed" and predicted that many would answer very simple and short answers. Another reviewer said it was ok since it would be easy to skip if they weren't comfortable with answering the question. Czaja and Blair (2005 in Andres 2012, 47) confirm that respondents of self-administered surveys are less likely to answer open-ended questions. In order to receive some level of idea of information security awareness, I felt the scaling options would be the best way to get an answer out of the respondents. Moreover, a deeper knowledge as to what they know about information security can be deducted from the questions following this one. It was important to ask this question before questions 8 and 9 as they would give clues as to what is considered information security and could bias the respondent's answer. This possibility, however, is not completely eliminated, as it is possible to move backwards in the survey.

In question 8, the most common information security threats that are presented in the theory part were listed and respondents were asked to consider their level of concern by rating on a scale of 0-4. A modification to the option set as 0 was made from "I don't think about it" to "I haven't thought about it" before the release of the survey. This was an important correction in order to establish the awareness as a continuance from question 7. In order to determine the relation of awareness and concern to means of protection, question 9 listed the main protective methods as options. Here it felt appropriate to add the open-ended option of 'other'. Finally question 10 allowed the respondents to share any

experiences related to the subject, which could also help determine the correlation between knowledge and action.

All questions went through a process of evaluation from a respondent and researcher point of view. The order, form and content of the questions were carefully considered. Andres (2012, 27) suggests that parts of and eventually the entire instrument should be pre-tested throughout the survey development process. Some reasons for this are to assess whether the language of the questions is appropriate for the audience, to ensure that the questions are understood as intended, to evaluate different versions of a question and to consider the order of the questions.

The survey was first reviewed by one of the thesis supervisors and some of the adjustments concerning the forming of questions were made at that stage. Later the commissioning party also shared their comments after which it was shared with three other people. Grammatical issues were fine-tuned by a philologist and specifications suggested from a user point of view were incorporated. After entering the questionnaire on Webropol and before the link was published, it was piloted by 2 different people within the target group and tested on Mac, Windows, iOS and Android platforms. Some corrections were still made at this stage.

4.3 Research sample

Lincoln and Guba (1985 in Andres 2012, 116) imply that the credibility of the study requires that it is “carried out in a way that ensures that the research participants are described and identified accurately”. The research participants in this case are the same as the target audience, which were described in more detail in chapter 2. The chosen respondents are young travellers who own a mobile device.

Although most sampling strategies involve generating lists of possible respondents, it is not necessary in all cases. Non-probability sampling allows the researcher to select the appropriate sample, for example convenience or availability samples that are easily accessible and able to take part in a survey research. (Andres 2012, 95-103) In this case, the group of friends on Facebook that are mobile device users, within a certain age group and travel at least once a year were chosen to participate in the study. This can also easily convert into a snowball sample as attendees may invite other friends that meet the criteria of the study. The aim was to collect at least 100 responses for the survey to be valid.

4.4 Data collection

An event on Facebook was created to which members of the sample group were invited. Individuals that met the criteria of the research were invited to the event and encouraged in the cover letter to invite their friends. At this stage, approximately 500 people were invited to partake in the survey. The final amount of invitees was hard to establish, as it was later shared on a Twitter account as well as passed on by email by some participants.

Creating an event instead of publishing it on a page helped to keep the sample group specified and to approach the respondents more directly and personally in order to increase the likeliness of completing the questionnaire. The name of the event included my name and the event picture was one from my previous travels and was recognizably myself. In this way, I attempted to make the invitation to the event and answering the survey more personal. Concerning the face validity of a study, Andres (2012, 116) establishes that "in survey research, often the first impression of a questionnaire, related cover letter and other materials will determine whether potential respondents will complete the survey". The cover letter was constructed keeping the target audience in mind (Appendix 2). It attempted to be light and playful yet including all the required information of a cover letter. The link to the survey was provided after relatively little information, in case a respondent did not find it necessary to look into the details. A similar introduction was repeated after following the link to the questionnaire (Appendix 1).

The event was published on Friday the 17th of April at 6pm. In general, many users are known to be online during the end of the week and weekend, which is why the survey was published at the selected time. Within 1,5 hours of the creation of the event and publication of the survey, half of the desired amount had responded. In one day, I had collected the required 100 responses. I had scheduled to keep the survey and event open for one week after which I would begin the analysis of the data. A reminder was published on the event page on Wednesday before which the amount of responses was at 173. By Friday the 24th of April, the amount of responses was already over double the initially aimed amount and the event was closed. The total amount of responses was 210.

As previously mentioned, the initial aim was to collect 100 responses. While creating an event allowed me to select the participants by inviting them to take part, no final records were shown as to how many people were invited in total, counting in the people other participants had invited to the event. An estimated amount according to comments from other participants notifying that they had invited more friends would be around 700 people invited altogether, out of which 210 filled in the survey. This would make the response rate roughly 30%. Online questionnaires have become ever more common due to the ease of

sharing through social networks, which has lead to lower response rates. Also, non-probability sampling through social networks aims to gather as high an amount of responses as possible, regardless of the overall sample it was open to.

5 Results

Once the theoretical framework was polished and the first part of the empirical section established, it was time to analyse the data. Webropol enabled the direct analysis and grouping of the responses. The answers were transferred to Excel and the figures and tables were formed to visualize the results. The questions and results have been divided into sections by relevant themes.

5.1 Demographic factors

Age, gender and nationality are considered as the demographic factors in this study. As predicted, the highest percentage of respondents were 25-years-old, representing 21,9% of all survey participants (Figure 3). The 24-, 26- and 27-year-old respondents were fairly close in response rates, whereas there were zero 19-year-olds, and only a few of responses from the age groups 18, 20, 21, and 32. This means that the answers cannot be very well generalized, as the age groups were not represented evenly. The results can be explained by the fact that the author of the survey herself was 25-years-old at the time, and so most of the people in her network are close to this age.

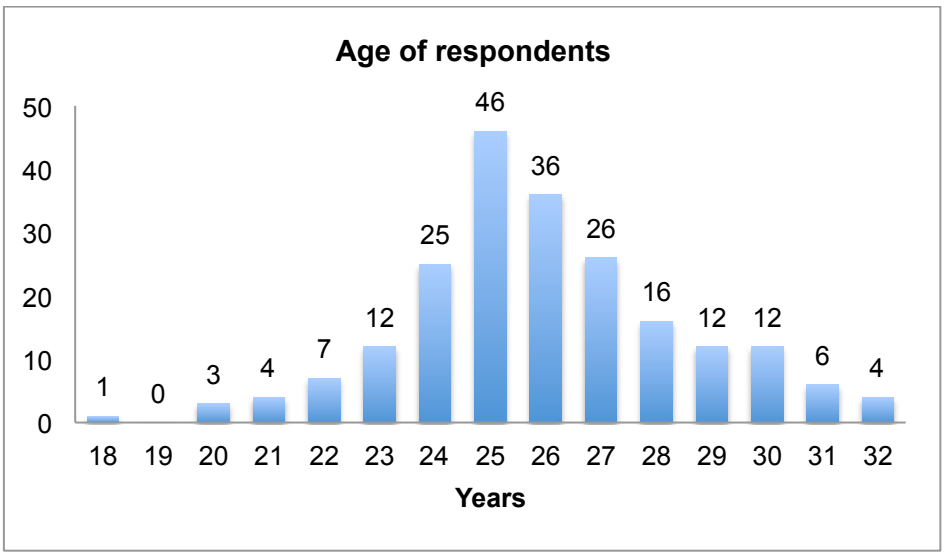


Figure 3. The age of the respondents of the survey (N=210)

The gender division was mostly female, as they represented 69,5% of the respondents (Table 1). This can also be explained as most of the researchers friends on Facebook, and invited research participants, are female.

Table 1. Gender division of respondents

Male	64	30%
Female	146	70%
Total	**210**	**100%**

Most survey takers were Finnish (68,6%), as is the researcher, yet a fair amount of variation was seen in the rest of the respondents (Table 2). There were respondents from 23 different countries. Most responses from these countries were collected from Brazil and Spain.

Table 2. Nationalities of the respondents of the survey (N=66)

Brazilian	13	**Slovakian**	1
Spanish	11	**Moldavian**	1
Russian	7	**Malaysia**	1
Greek	5	**Latvian**	1
Canadian	4	**Kuwaiti**	1
American	4	**Italian**	1
Polish	2	**Indian**	1
Mexican	2	**German**	1
French	2	**Dutch**	1
Estonian	2	**Belgian**	1
British	2	**Austrian**	1
South Korean	1		

This diversity results from time spent abroad by the maker of the survey as a high school and Erasmus exchange student and connecting with friends all around the world.

5.2 Respondents' travel habits

Exactly half of the respondents travel one to two times per year (50%) and second to most three to five times per year (38,1%). 10,5% of all respondents were more frequent travellers who travel over five times a year (Figure 4).

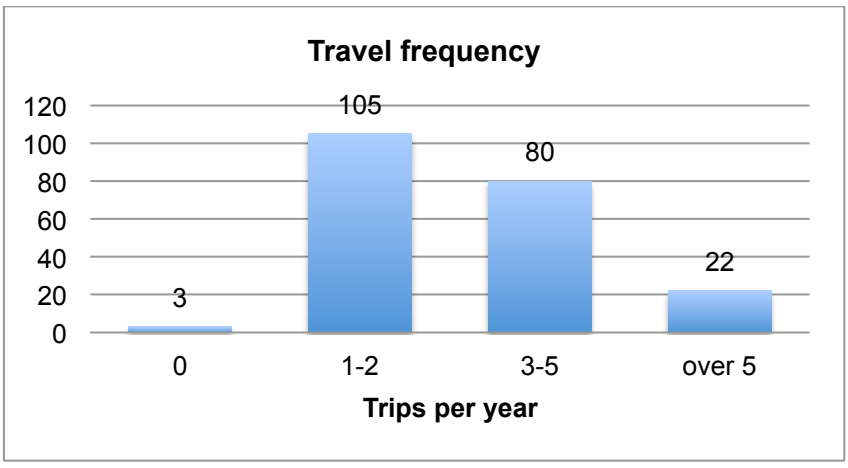


Figure 4. Trips per year abroad (N=210)

Merely three respondents (1,4%) responded zero, which can mean that they travel less frequently than once a year or not at all. This group of people were not excluded from the study due to the interpretation of the question and minimum affect to the results. The small amount can reflect on the significance of the age group to the travel industry, as

most people who consider themselves as “travellers”, travel well over once a year. On the other hand, the research participants were summoned as “young travellers” so it may be that some potential respondents did not fill in the survey because they did not feel they fit the criteria despite having travelled at some point. There were no major differences in responses between genders.

Almost all participants of the survey carried a smartphone with them when they travel (95,7%). Over one quarter had touchscreen tablets (26,2%) and even more said they took laptops with them (34,8%) (Figure 5).

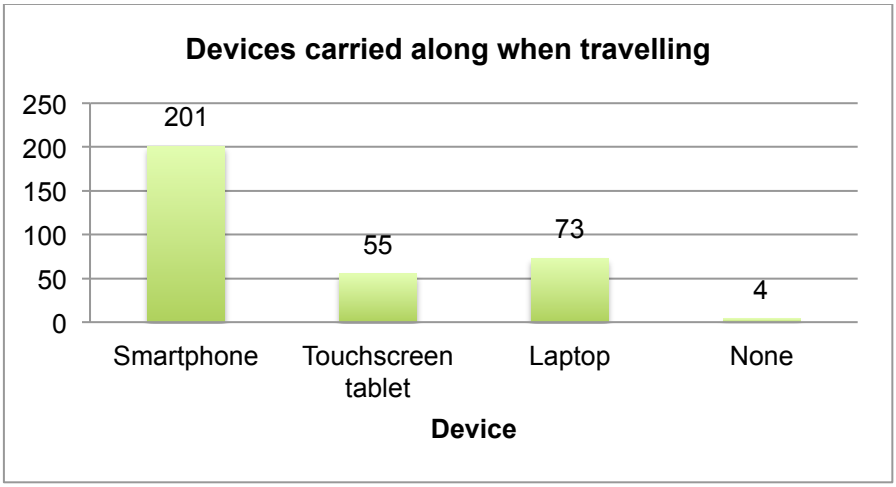
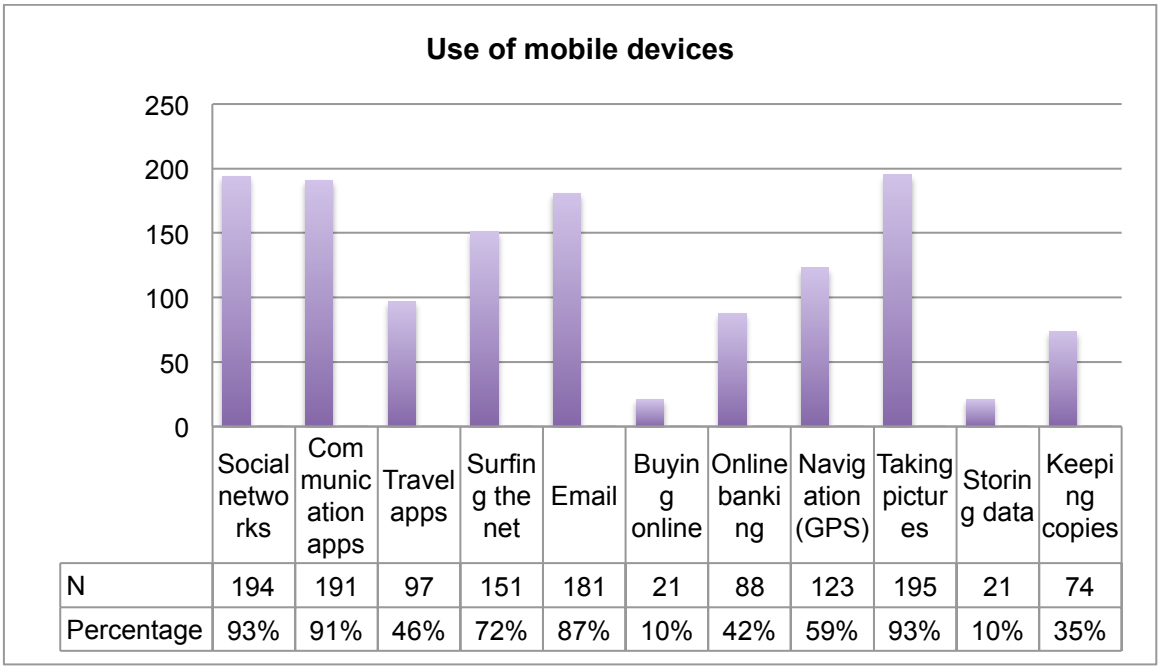


Figure 5. Devices respondents take with them when travelling (N=210)

Again, merely 2% did not carry any of the aforementioned devices. All respondents that carried a tablet or a laptop with them also had a smartphone. 18 respondents carried all three devices when travelling (8,6%).

5.3 Young travellers’ use of mobile devices

The most common use for the aforementioned devices were online social networks (92,8%), communication apps (91,4%), email (86,6%) and taking pictures (93,3%) (Figure 6). Most of these require access to the internet and so potentially predispose all other information stored on the device, such as the pictures taken.



	Social networks	Communication apps	Travel apps	Surfing the net	Email	Buying online	Online banking	Navigation (GPS)	Taking pictures	Storing data	Keeping copies
N	194	191	97	151	181	21	88	123	195	21	74
Percentage	93%	91%	46%	72%	87%	10%	42%	59%	93%	10%	35%

Figure 6. Activities used on mobile devices by respondents when travelling (N=209)

Up to 35,4% kept copies of passports and other travel documents on their device(s) and 10,1% stored usernames and passwords on them. This means that over one third store sensitive data such as passport information and every tenth person extremely sensitive data, such as usernames and passwords, on their device(s). Similarly, one in every ten people bought goods and services online (10,1%). Moreover, 42,1% did online banking during their trips. Rather surprisingly, less than half of the respondents used travel apps (46,4%) during their travels, which means that they are not yet as common amongst travellers as previously suspected.

5.4 Level of awareness of information security

Almost half of the respondents did not feel very well informed of information security risks (48,1%) and one tenth did not feel like they were at all informed (10,5%), making almost 60% of respondents insecure of their awareness of information security. Only one in 20 felt very well informed (5,7%) and over one third felt fairly well informed (35,7%).

In general, the male respondents felt more informed of information security risks (Figure 7). 14,1% of men felt very well informed where the corresponding percentage for women was only 2,1%. Similarly, only 4,7% of male respondents and up to 13% of female respondents did not feel at all informed.

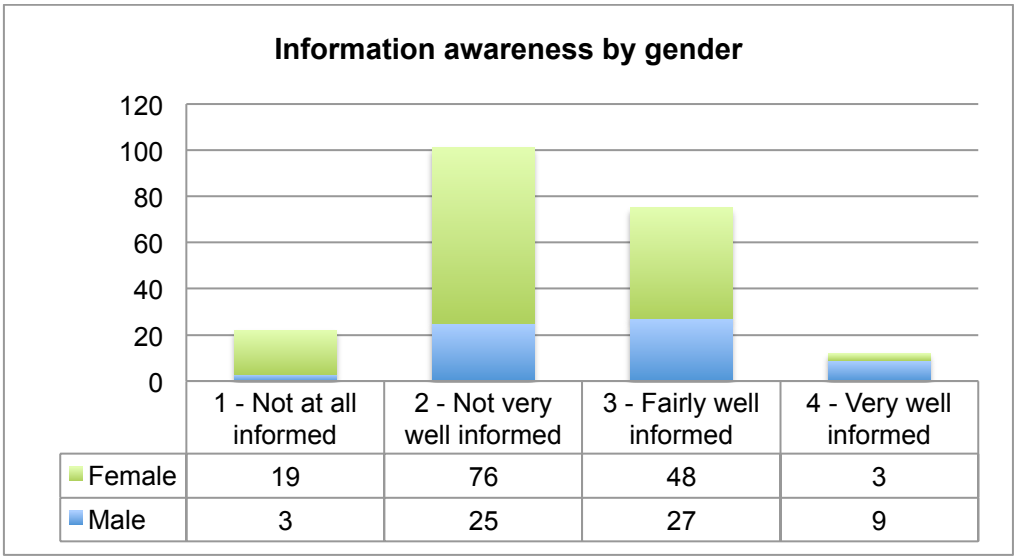


Figure 7. Awareness of information security by gender (N=210)

Of the 22 respondents who did not feel at all informed exactly half were Finnish, which is 7,7% of all Finnish respondents whereas the respective number for respondents of other nationalities is 16,7%. However, of the 12 that felt very well informed, 10 were Finnish and only 2 from other nationalities. If generalizable, this could mean that Finnish people are generally more aware of information security.

5.5 Concerns of risks in information security

Generally, most respondents were at least somewhat concerned about all of the listed risks. There was also mainly higher concern than no concern at all (Figure 8).

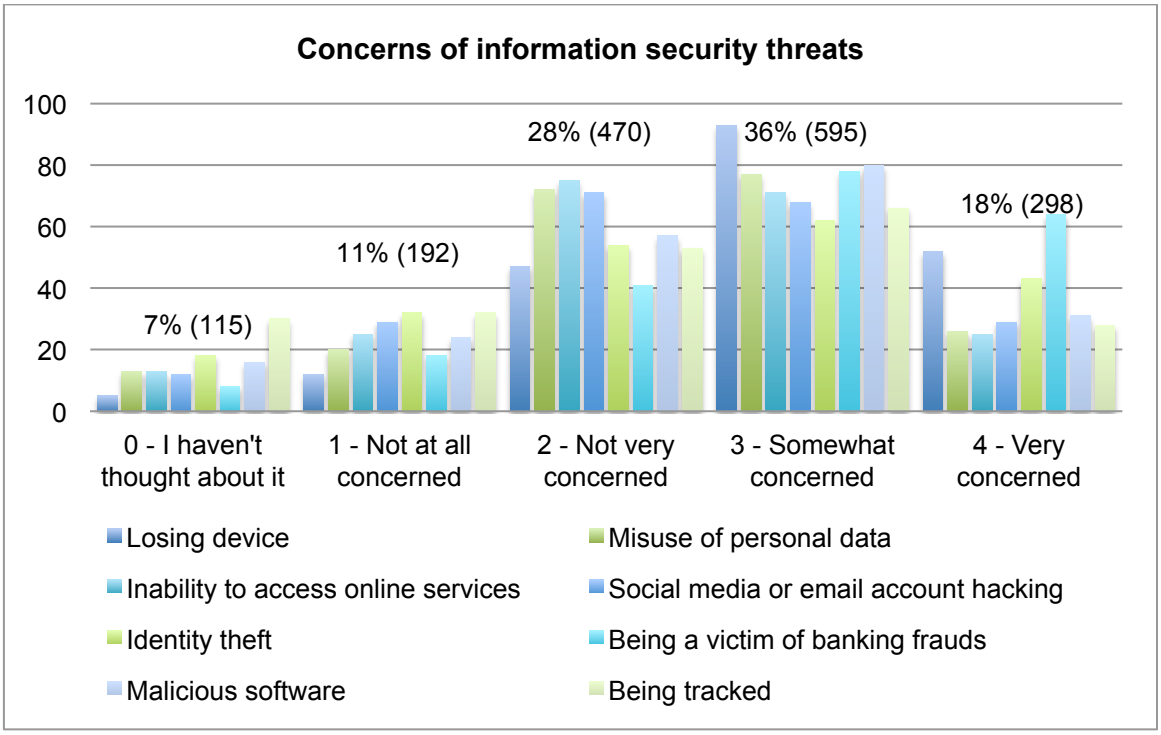


Figure 8. Respondents' levels of concern of information security threats (N=210)

The highest concerns were losing a device and becoming a victim of bankcard or online banking fraud. Almost 70% were somewhat or very concerned about losing their device (69,4%); specifically 44,5% somewhat concerned and 24,9% very concerned of losing their device. Equivalently, 67,9% were somewhat or very concerned of becoming a victim of banking card (37,3%) or online banking fraud (30,6%). These two threats are the most concrete risks to the user of a mobile device because they are directly related to material or financial loss, which explains the high rates of concern. Specific numbers and percentage are presented in graphs in the appendix of this thesis, each threat presented as its own (Appendix 3).

Two options showed identical results. These were concerns over not being able to access online services or a social media or email account being hacked (Appendix 3). Around 30% were not very concerned and the same amount were somewhat concerned. Similarly, there was the exact same amount of people who were not at all concerned as there were people who were very concerned about these two issues; 12,0% with regard to an inability to access online services and 13,9% concerning account hacking. Around 6% for both options had not even thought about it. The similarity of the results can indicate that the two options were too similar from the respondent point-of-view. They may associate inability to access online services with hacking, or vice versa. Online services and own accounts may also seem like equivalent terms to the respondent.

Identity theft as a threat was of highest concern to every fifth respondent (20,6%), and the third most concerning of all threats. Up to 8,6% had not even thought about it, which made it the second to most unconsidered threat. Over half of the respondents (53,4%) were somewhat or very concerned about discovering malicious software on their devices, specifically 38,5% somewhat and 14,9% very concerned. The most unthought-of threat was being tracked. 14,4% said they had never considered the threat of being tracked and a similar amount of respondents were not at all concerned (15,3%), yet almost every third was somewhat concerned about it (31,6%).

In relation to the overall average, no significant differences occurred between respondents who had previously said they felt fairly well informed and those who didn’t feel very well informed (Table 3). These two middle groups represent 83,8% of the respondents, specifically 48,1% not very well informed and 35,7% fairly well informed as discussed previously. This means that most responses of these two groups reflect the average values.

Table 3. Level of awareness vs. level of concern of respondents (N=210)

Respondents	Haven't thought about it	Not at all concerned	Not very concerned	Somewhat concerned	Very concerned	%	N
All	**7%**	**12%**	**28%**	**36%**	**18%**	**100%**	**209**
Not at all informed	**13%**	**9%**	**24%**	**30%**	**24%**	**100%**	**22**
Not very well informed	7%	10%	28%	38%	17%	100%	100
Fairly well informed	5%	14%	31%	35%	15%	100%	75
Very well informed	**7%**	**16%**	**21%**	**27%**	**28%**	**100%**	**12**

However, differences are quite distinct between the two extremes. Almost double the amount of respondents in the group 'not at all informed' hadn't thought about most of the options compared to the group 'very well informed' (12,5% vs 7,4%). Similarly, there were close to double the respondents in the 'very well informed' who were not at all concerned about most threats, in comparison to the 'not at all informed' (15,8% vs 9,1%). Rather surprisingly though, the levels of higher concern were fairly similar between the two groups; somewhat concerned 29,6% and 27,4% and very concerned 24,4% and 28,4% for the 'not at all informed' and 'very well informed' respectively. Still the more informed felt faintly more concerned of most threats. These results could indicate that the more the respondents were aware of the risks, the more concerned they were about certain risks. Equally, they were less concerned of risks that were considered smaller. In this part of the survey, the questions could have been ranked according to levels of threat, from smallest to biggest or vice versa, in order to allow for further analysis of the results and behaviours.

However, a distinctive characteristic of the groups that felt less aware of the risks was that they focused more on the middle options of the scale compared to the very informed, which indicates that they are less sure of the risks at hand.

5.6 Current data security measures

195 of the 210 respondents answered this question, which means 15 respondents did not take any security measures while travelling (7,14%) (Figure 9). The most common privacy measure taken by the respondents was using a passcode to restrict access to their device(s) (83,3%). Up to 41% of the respondents had antivirus software installed on their device and every third made sure apps and software were up to date before travelling (34,3%).

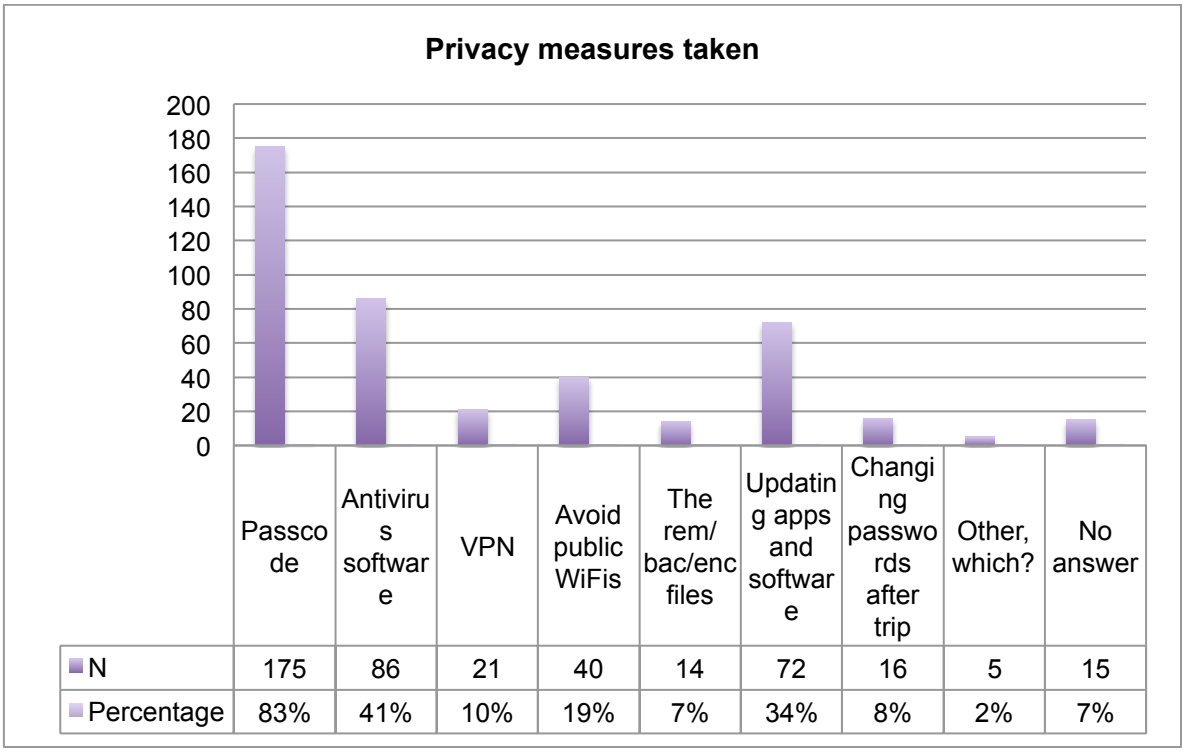


Figure 9. Privacy measures taken on devices by respondents (N=210)

Just under every fifth respondent said they avoided public WiFis (19,1%) and only every tenth had a VPN in use (10,0%). The rest of the options remained around 7%. Most answers concerning the removing, backing up or encryption of data specified making backups as the precaution taken, whilst only one specified removal and one encryption. In addition, there was one clear misconception of the question as the answer “photos and notes” indicated the type of data handled.

Five respondents used other security measures (2,4%), which were listed as the following:

- “complete viruscheck after returning”
- “I keep my phone on my person or in my immediate vicinity at all times.“
- “i try to buy as less as possible , trough the net.”
- “I don´t carry all my data with me when i travel”
- “I don't take my devices eveywhere, like in Finland. I might leave them in the hotel room safe and just use them at the hotel.”

The first answer, completing a virus check after returning, is a very relevant option to security measures and a good addition to the list as it was also mentioned in the theory part. Similarly, the last open-ended response can be a valid measure for securing a device, though it does not allow the user to benefit from the convenience of the device when travelling. However, the second answer to the open question indicates that the respondent is not entirely aware of the main risks to information security. As discussed in the theory part, the device does not need to leave the owners possession for data to become predis-

posed to threats. The two other options were already incorporated in the questions and options of the survey and simply highlight their relevance.

Out of the respondents that felt very informed of information security, all of them used at least a passcode to restrict access to their device. Half of them also had antivirus software and avoided connecting to public WiFis when travelling. Every fourth used a VPN, removed, backed-up or encrypted files before travelling, made sure all apps and software were updated and changed passwords upon return (Table 4).

Table 4. Level of awareness vs. security measures taken (N=210)

Respondents	Passcode	Antivirus software	VPN	Avoid public WiFis	Removing/ backing up/ encrypting files
All	**83%**	**41%**	**10%**	**19%**	**7%**
Not at all informed	**82%**	**23%**	**14%**	**0%**	**9%**
Not very well informed	80%	37%	4%	18%	3%
Fairly well informed	85%	51%	15%	21%	9%
Very well informed	**100%**	**50%**	**25%**	**50%**	**17%**

	Updating apps and software	Changing passwords after trip	Other, which?	No answer	N
All	**34%**	**8%**	**2%**	**7,14%**	**210**
Not at all informed	**23%**	**5%**	**0%**	**13,64%**	**22**
Not very well informed	34%	3%	2%	7,92%	101
Fairly well informed	40%	12%	3%	5,33%	75
Very well informed	**25%**	**25%**	**8%**	**0%**	**12**

Only 86,3% of the respondents who did not feel at all informed responded to this question of which 81,8% used a passcode to restrict access to their device(s). None of them said they avoided public WiFis, and merely 4,5% changed passwords, yet up to 13,6% used a VPN. This group had the highest non-response rate in this group, as 13,6% did not choose any of the options, indicating that they do not use any measures to protect their data. Here it is clear that the percentage of people who did not use any of the listed security measures decrease towards the more informed, seeing as all respondents of the very well informed responded to the question.

In general, there was an ascent to measures taken towards the more informed. It is most defined in avoiding public WiFis, but can also be seen in using passcodes, having antivirus software, and changing passwords. A deviation occurs in updating apps and software, as the 'very well informed' have generally a lower rate of response. The respondents in the group of 'very well informed' are few, so each response is highlighted and gives a very caricatured generalisation, which may be the issue in this particular option.

5.7 Past experiences

There were 60 responses (28,6%) to this final, open-ended question asking whether the respondents had any personal experiences related to information security loss (Appendix 4). Most of them simply stated ‘no’ with some comments of the sort ‘not yet at least’ and ‘I consider myself very lucky!’ Many indicated that they realized it could still be a concern in the future.

Some answers however included very descriptive accounts of events, such as the following respondent who had their phone stolen:

> “My phone was stolen once and I felt quite exposed. I lost all my contacts and pictures. And I immediately changed my email and social networking account passwords. I didn't go to the police as it is impossible to find a phone after it's stolen, and police do not actively search for it. Nowadays, I copy or move photos and contacts to another location when my phone gets full. I also delete photos I have moved from my phone.”

In this answer, it becomes clear that previous experiences have affected security measures today, and the respondent felt that their privacy was breached. In many cases respondents have tightened security measures and have realized the vulnerability of their information only after such an event. Further, some other examples of physical loss imply the same:

> “My smartphone got stolen a couple of years ago in Spain. I immediately called my brother in Finland and he changed all my passwords (to gmail, facebook...). It scared me how easy it actually is to use someone others phone with only breaking the pincode/screencode. After that you can access everything without passwords.”

> “Someone stole my phone and I used to have all my nip's of my credit and debit card in some notes. So I have to called the bank and ask for call in every charge I made.”

> “Phone stolen along with ID and debit card (in Finland). Thieves got access to personal information including finding out my home address. They managed to call paid sex lines etc before I cancelled the line and I had to pay the 300+ euro bill (insurance wouldn't cover). Phone was not a smartphone. Perhaps a phone with a lock screen could've prevented this.
> They also used my personal information to order large, expensive things online for home delivery as a prank. These included a buggy and gym equipment which thank-

> fully weren't paid for. I had to cancel anything else they might be able to abuse with access to all my personal info, such as library cards etc."

This last experience conveys the severity of losing a device and the financial losses that easily occur with them. The following experiences describe the immaterial losses and the consequences of hacking:

> "Somebody hacked my pc once and use my IP to open fake account on eBay."

> "On my last trip abroad, my main email account was hacked and someone changed my password. I had to create a new one and lost all my contacts."

> "My laptop was hacked while I was in university using a public network. The hacker took one of my essays and handed it in to the prof as their own. Fortunatly, the hacker came clean and stated the essay wasn't hers. When I found out I had been hacked, I immediately researched ways to decrease any risks of being hacked... especially that I had plenty of personal data on my computer. Who knows what else was taken from me. All passwords have now been changed and my firewall and other security/privacy settings have been updated to the maximum security possible!"

The second example demonstrates the exposure of not only ones own information, but those of others. Also, the respondent certainly lost a vast amount of valuable information and had to spend time in gathering contact information in the future. The last of the three describes a very concrete course of events. In this case, the hacker was in the same social circles as the respondent, which demonstrates how easy it is for anyone to reach another persons files through a shared public network. Secondly, it was a seemingly "safe" network, which is usually protected from outer exposure and requires passwords. Finally, the victim had no way of knowing what else was stolen and started researching ways of preventing it from happening again. The hovering feeling of insecurity and what other information continues to be exposed is one of the most concerning aspects of information security loss. A final extract of the open answers addresses the demand for post-security measures.

> "My phone had got stolen before and I'm worrying that the theft or whoever is using my phone can see my photo through iCloud. That's why now I logged out from iCloud and stop syncing my photos. It would be nice to know if there is a way out from this trouble though."

Many good yet unfortunate examples were gathered through this open-ended question. However, as it was stated in the theoretical part, the victim is not always aware of stolen

data since it in some cases it is not lost but copied, so there could still be many who are simply not aware of being victims of data theft.

5.8 Summary of results

There were 210 respondents with a response rate of roughly 30%. The exact response rate could not be established due to the chosen research methods and focus on gathering a valid amount of responses from a large open network.

Most responses came from 25-year-old respondents and the average age was 26. Almost 70% were female and 30% male and 70% were of Finnish nationality and the rest represented 23 different nationalities. Half of the respondents travel 1-2 times per year and up to 40% travel 3-5 times per year abroad. Almost all respondents carry a smartphone with them and roughly half of them carried more than one device.

Respondents use their devices most to take pictures, log in to online social networks and use communication apps. 60% of all respondents do not feel very or at all informed of security risks and male respondents are generally more confident about their awareness.

Mostly respondents were at least somewhat concerned of the listed information security risks. The highest concern occurred in physical loss such as losing a device or financial losses. The least considered risk was that of getting tracked. The results are most distinct when comparing the two extremes of information security awareness. Generally, the respondents who felt very aware of the risks were more concerned of certain risks and less concerned of risks they considered smaller. In other words, they were more decisive in the two extremes of concern. 13% of the respondents who did not feel at all aware of risks had not even considered most of the risks.

The most used security measure was using a passcode. The results indicated that the more aware the respondent was about information security risks, the more and higher rates of security measures they took. The final open-ended answers provided good examples regarding the possibilities of data vulnerability. Many who had already been a victim of data loss had reacted fast and changed information security behaviour.

6 Discussion

This final chapter will present the results of the survey and research as a whole. The thesis and research process will be evaluated by considering its validity and reliability, and further research suggestions will be provided.

6.1 Overview and conclusions of the study

After the results and analysis of the research, the hypotheses can now be considered either supported or not supported by the study (Bell and Waters 2014, 34), or accepted or rejected. This requires assessing the level of confidence one feels they can have about making valid inferences about the population of the sample data so as to assess the validity of the results. (Brotherton 2008, 195)

The validity of the generalizability of the sample group in this study is considered by reflecting on the size of the sample group, as the response rate could not be specifically determined due to the chosen methods. However, the desired amount of responses were collected and doubled, which specifically implies that the sample group for this research can be considered valid. The quality of the sample group can be analysed with the results. As established, all the age groups within the study were not evenly represented, so the results cannot be generalised to the entire population. The majority of the respondents were between 23 and 30 years, and so the results could better reflect a narrower age group. The distribution between women and men were 70% vs 30%, as well as for the nationalities of Finnish and other. This should be taken in consideration when further applying the results.

However, the collection methods through Facebook permitted reaching the correct target group, as they were essentially young mobile device users who travel. Moreover, it has been established that the age group is the most active in social media and have the highest rates in owning a mobile device. This minimized the margin for error in the quality of the sample group. The results in fact confirmed this as less than 2% had either travelled less than once a year and the same amount did not own a mobile device and so the overall results remained uncompromised. In addition, the data was collected automatically with the Webropol software, which ensured the integrity of the data collected.

The question of mobile device usage confirmed that people do not necessarily minimize the use of their devices and connecting to their social networks when they travel as many of the provided options of use reached over 90%. Just under half of the respondents used travel apps though, which means that travel apps have yet to reach their potential. The

question also helped establish that still quite a few carry sensitive and valuable data on their devices, even when travelling.

Although the question 'how well informed do you feel' attempted to ease the answering of the question, the answers depended highly on the respondent's own consideration. One might feel insecure of their knowledge though it may be higher than one that is very confident of their own awareness. Nevertheless, it was distinguishable that most respondents did not feel very aware of information security risks. The results of this question therefore **support** the first hypothesis of the research, **hypothesis A, "the young traveller lacks knowledge of the current information security risks".**

The intention of the following question, "how concerned are you about the following risks regarding information security", was to additionally confirm this hypothesis. The results showed mainly high levels of concern in general amongst the sample group. The group of people who had not thought about most of the risks remained at around 7% although it was clearly higher amongst the not at all informed (13%). The indecisiveness and hovering around the mid-values could suggest that people are not certain of what the risks specifically are in each case, and therefore were indifferent of them, whereas it could be seen that the group of 'very well informed' were more clear about their concern or lack of concern, in which case the hypothesis would be further supported.

The results of the question asking what privacy measures people are currently taking determined whether the second hypothesis, hypothesis B **"the young traveller is not securing his or her data"**, is accepted or not. Though over 80% use passcodes to limit access to their devices, the implementation of the rest of the security measures remained under 35% with most under 10%. Surprisingly though, up to 41% had antivirus software installed on their mobile devices, although it is considered less common than having them installed on a PC. Still, taking into consideration the overall, low levels of privacy measures taken, **hypothesis B** is also **supported** by the results.

At this stage it can be determined whether the primary objective was reached. This means that the results were informative and trustworthy so that the commissioner could benefit from them. Overall, the results from the sample group could be generalizable, considering the demographic factors and representation, and within the scope and delimitation of the thesis. Awareness remains low amongst young travellers and usability of mobile devices high, which means that in order to be able to reach the target audience, awareness should be raised amongst them. Though current events and news regarding information security are common and frequent, the commissioning party could better target their message by reaching out to the tourism industry and focusing a part of their marketing on services

most often used by travellers such as airports, travel sites, travel agencies, etc. Marketing material should also focus on building awareness of the threats directed at travellers. In terms of product development, an application directed at the young traveller could become useful as long as the target audience becomes aware of its necessity. It could provide information on threats and alerts concerning the security of a public WiFi, or it could even be a package of the available products, which could be a combination of products focusing on the needs of a traveller.

The final hypothesis involves the assessing of the two previous hypotheses as variables and whether they are in some way correlated. The two variables were awareness and the protection of data. The correlation of the two was examined in the final parts of the results, where levels of awareness were cross-examined with current measures of protecting data, as well as considering the answers of the open-ended questions regarding previous experiences. The results specifically showed an inclination on measures taken towards the level of awareness amongst the respondents, which confirmed that the two variables are correlated. Furthermore, the open-ended questions pointed out that own experiences raised awareness of information security and consequently added to measures of data protection. **Hypothesis C, "the level of awareness of current information security risks of the young traveller affects whether he/she protects his/her data",** is therefore **accepted** and highlights necessity of raising awareness in order to increase demand amongst consumers.

In general, I received good feedback from the questionnaire from people saying that it was simple enough and easy to answer as well as gratitude for it actually taking the short time I claimed it would. Some even came to me and said that they felt bad after answering it as they realized how hopeless they were about the issues covered in the questionnaire. The only jargon they were confused about was VPN, which did not affect the validity of the results, as it was clear that if the respondent did not know what it was, they would not be using it as a security measure. There were even a few that mentioned they were interested in reading the final report and learning more about information security.

6.2 Direction for further research

In continuance of the suggestions following the research for the commissioning party, it would be relevant to study what are the most common sites where travellers seek information and what kind of ads they pay attention to when travelling. This could also include examining how they prepare for a trip and whether they look for advice online and concerning what issues particularly. The study could focus on whether they look for security advice in general and what should be taken into consideration.

Another option would be to find out what information tour operators and travel agencies provide concerning security during trips and how they could cooperate with information security companies: whether they could resell products such as VPN or antivirus software in a similar way to additional insurance.

Deeper analysis to this particular topic could include the variability of different age groups and the proneness to tightening security measures along with the awareness of the risks. The studied age group in this study was inevitably more aware of certain security issues as they are more frequent users of the mobile device. It would have also been interesting to include the educational and professional backgrounds of respondents and discover how it affected the awareness. IT is a very common field of study and industry nowadays, and the issues have certainly been handled within the program. Also, businesses are looking into the measures of information security of their employees as they carry a lot of corporate secrets. Information security training has recently become a part of the induction of new employees.

6.3 Thesis process and learning

It was paramount for me to find a topic that would fit into the standards of a good topic for a thesis presented by the university. This was not only for the purpose of meeting the prerequisites provided by the university but they were standards that would ensure my interest and motivation throughout the process of the thesis. I strongly believed that by combining the knowledge I have from my education with the knowledge I could obtain from my current work place, I would achieve a topic that would be comprised of both. The hardest part was finding that topic. As soon as I had found it, it was easier to find the determination as well. The second hardest part was to define the research problem and narrow it down. Once it was clear and decided on, I could establish a strict timetable and small goals in order to finish the thesis in time.

I started off with the theoretical part and found that luckily there was astonishingly much information about the topic. I was also positively surprised that the information was so current. Complications occurred when I found that the sources went too deep into the topic and I could not possibly cover it all, along with the vast amount of information I had already gathered. Slowly the pieces fell into place and I realized I had to give up on the attempt to include everything I had initially planned to.

I felt the making of the survey felt natural and simple at the time, as I studied many examples and kept it within the realms of the theoretical part. The gathering also went smoothly and I felt that the work was almost done. However, when it was time to look at the results and tools at hand, I almost fell into despair. Again I wasn’t sure how deep into the analysis

of the data I was supposed to go, as there were options to twist and turn them in every way possible. I soon found comfort in realizing the scope of a thesis at this level did not require covering all those terms that were at my disposal. I decided to use my own judgment and Excel skills to analyze what was most relevant for the study, as one of my initial objectives for the thesis was to keep it sweet and simple, so to say.

Overall I feel that once the initial obstacles were beat, it was a relatively smooth process. In particular the writing process felt more natural towards the end. Connecting the field of my current work place with the field of my studies kept me interested in the topic throughout the process. It was valuable for me to learn more about the company I work for and grow as an employee, while simultaneously introducing something new to my studies.

6.4 Comments from the commissioner

Once the thesis was prepared for presentation, it was handed over to the commissioner to examine. At this stage, some comments were provided and it was requested that they were included in the thesis proper.

Overall, the commissioner was very pleased with the thesis and expectations were even exceeded to some extent. Praise was given to the structure and layout of the research along with the written expression. The commissioner also agreed with the results and was certain that they would be of use to the company. Only minor notes were directed at some issues in content, such as it was initially stated that the research was purely quantitative when in fact qualitative data was also included and analyzed. This was later adjusted in the thesis.

The true value and use of the thesis could not yet be entirely determined though plans to apply the thesis to corporate use have been made in terms of marketing and public relations. Furthermore, suggestions to producing a scholarly article of the research were proposed. Use for product developments have not yet been discussed.

References

Andres, L. 2012. Designing & doing survey research. SAGE Publications Ltd. London

Bell, J. & Waters, S. 2014. Doing your research project. 6th ed. McGraw-Hill Education. Berkshire

Blevins, B. 11 Feb 2014. For international travelers, is basic business data security enough? URL: http://searchsecurity.techtarget.com/news/2240214203/For-international-travelers-is-basic-business-data-security-enough. Accessed: 12 April 2015

Brotherton, B. 2008. Researching hospitality and tourism. SAGE Publications Ltd. London

Clack, D. 2015. The world's 50 best travel apps. URL: http://www.timeout.com/travel/features/1169/the-worlds-50-best-travel-apps. Accessed: 27 April 2015

Crossland, K. 29 Jan 2014a. 5 big privacy problems that come with big data. URL: http://www.techopedia.com/2/29682/trends/big-data/5-big-privacy-problems-that-come-with-big-data. Accessed: 15 April 2015

Crossland, K. 14 Oct 2014b. Web roundup: Smartphones, hackers and cutting-edge mobile technology. URL: http://www.techopedia.com/2/30904/in-the-news/web-roundup-smartphones-hackers-and-cutting-edge-mobile-technology. Accessed: 15 April 2015

Crossland, K. 11 Nov 2014c. Web roundup: Security remains a top concern. URL: http://www.techopedia.com/2/30975/in-the-news/web-roundup-security-remains-a-top-concern. Accessed: 15 April 2015

Dickinson, J.E., Ghali, K., Cherrett, T., Speed, C., Davies & N., Norgate, S. 2014. Tourism and the smartphone app: capabilities, emerging practice and scope in the travel domain. Current issues in tourism. 17, 1, 84-101. URL: http://eprints.bournemouth.ac.uk/21155/1/Dickinson%20et%20al%202013%20Current%20Issues.pdf. Accessed: 12 April 2015

Drevin, L., Kruger, H.A, & Steyn, T. 2006. Value-focused assessment of ICT security awareness in an academic environment. Computers & security. Elsevier Ltd. February 2007, 26, pp. 36-43

eMarketer. 15 Jan 2013. ‘Generation Y’ leads the way on smartphones. URL: http://www.emarketer.com/Article/Generation-Y-Leads-Way-on-Smartphones/1009604#6KkhKEIrRXAxTYH2.99. Accessed: 6 April 2015

Emory University 2015. Information security travel tips. Emory Libraries & Information Technology. URL: http://it.emory.edu/security/travel.html. Accessed: 13 March 2015

European Union 2015. Special Eurobarometer 423 “Cyber Security”. European Commission. URL: http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf. Accessed: 9 April 2015

Franklin, M.I. 2012. Understanding research. Coping with quantitative-qualitative divide. Routledge. Oxon

F-Secure 2014. Essential, simple tips to ensure your online safety & privacy. URL: https://www.f-secure.com/en_GB/web/press_gb/news/news-archive/-/journal_content/56/1082184/1095189?p_p_auth=TW2CBVwo&refererPlid=910425. Accessed: 31 March 2015

F-Secure 2015a. F-Secure expert says VPNs are a vital accessory for Easter travellers. URL: https://www.f-secure.com/en_GB/web/press_gb/news-clippings/-/journal_content/56/1082184/1220143?p_p_auth=NnAc7soi&refererPlid=910425. Accessed: 31 March 2015

F-Secure 2015b. Is our online future worth sacrificing our privacy and security? URL: http://privacy.f-secure.com/2015/04/30/is-our-online-future-worth-sacrificing-our-privacy-and-security-rp15-2. Accessed 15 May 2015

F-Secure 2015c. Company web pages. URL: https://www.f-secure.com/en. Accessed: 21 April 2015

Furnell S. 2006. IFIP workshop - information security culture. Computers & Security. Elsevier Ltd. February 2007, 26, pp. 35

Gibson, R. 31 Mar 2013. Generation Y characteristics. URL: http://www.generationy.com/characteristics. Accessed: 30 April 2015

Heikkilä, T. 2008. Tilastollinen tutkimus. 7th ed. Edita Prima Oy. Helsinki

Järvinen, P. 2012. Arjen tietoturva - vinkit ja ratkaisut. Docendo. Jyväskylä

Manglis, A. 2010. Challenges and opportunities for the use of mobile applications in tourism. Europe INNOVA, MOBIP Project. URL: http://www.atlantisresearch.gr/files/Mobile_Applications_in_Tourism.pdf. Accessed: 27 April 2015

McMullen, J.F. 12 Nov 2014. Who owns all the data collected about you? The Answer May Surprise You. URL: http://www.techopedia.com/2/30973/trends/who-owns-your-information. Accessed: 15 April 2015

Mortleman, D. 2009. Top five data security travel issues: Protect sensitive information on business trips. URL: http://www.computerweekly.com/feature/Top-five-data-security-travel-issues-Protect-sensitive-information-on-business-trips. Accessed: 13 March 2015

Pound, W. 2009. Infosec 2009: How to beat airport data theft threat. URL: http://www.computerweekly.com/news/1280096893/Infosec-2009-How-to-beat-airport-data-theft-threat. Accessed: 12 April 2015

Rousku, K. 2014. Kyberturvaopas. Tietoturvaa kotona ja työpaikalla. Talentum Media Oy. Helsinki

Safe & Savvy. 27 Nov 2013. Yes, you do have something to hide. F-Secure. URL: http://safeandsavvy.f-secure.com/2013/11/27/yes-you-do-have-something-to-hide. Accessed: 9 April 2015

Safe & Savvy. 24 Jun 2014. 11 ways to stay safe online when you're travelling. F-Secure. URL: http://safeandsavvy.f-secure.com/2014/06/24/11-ways-to-stay-safe-online-when-youre-traveling. Accessed: 28 April 2015

Safe & Savvy. 23 Mar 2015a. 5 things you need to know about securing our future. F-Secure. URL: http://safeandsavvy.f-secure.com/2015/03/23/5-things-you-need-to-know-about-securing-our-future. Accessed: 10 April 2015

Safe & Savvy. 2 Apr 2015b. 3 mobile security tips for travellers. F-Secure. URL: http://safeandsavvy.f-secure.com/2015/04/02/3-mobile-security-tips-for-travelers. Accessed: 9 April 2015

Safe & Savvy. 1 May 2015c. The one question that could change the privacy debate. F-Secure. URL: http://safeandsavvy.f-secure.com/2015/05/01/the-one-question-that-could-change-the-privacy-debate. Accessed: 15 May 2015

Student Marketing 2015. Market overview and trends. URL: http://www.student-market.com/youth-travel. Accessed: 24 April 2015

Tamarov, M. 25 Mar 2015. Study finds lack of investment in mobile app security. URL: http://searchsecurity.techtarget.com/news/4500243095/Study-finds-lack-of-investment-in-mobile-app-security. Accessed: 12 April 2015

Tchacos, A. 4 May 2012. The travel generation. URL: http://inkwirenews.com.au/2012/05/04/the-travel-generation. Accessed: 6 March 2015

Tranberg, P. & Heuer S. 2013. Älä kerro kaikkea! Itsepuolustusopas verkkoon. Talentum Media Oy. Helsinki

Tourism Business Portal 2015. What tourism apps for mobile devices could be of interest to my client. URL: http://ec.europa.eu/enterprise/sectors/tourism/tourism-business-portal/documents/toolstutorials/positioning/tourism_apps.pdf. Accessed: 27 April 2015

UNWTO. 2015a. UNWTO World Tourism Barometer. Volume 13. Madrid. URL: http://dtxtq4w60xqpw.cloudfront.net/sites/all/files/pdf/unwto_barom15_02_april_excerpt__0.pdf. Accessed: 24 April 2015

UNWTO. 2015b. Why tourism? URL: http://www2.unwto.org/content/why-tourism. Accessed: 25 April 2015

Van den Berg, J. 14 Oct 2013. Millenials & social media: The what, where and why [infographic]. URL: http://www.insites-consulting.com/infographic-millennials-social-media. Accessed: 15 May 2015

Van Vaals, F. 2013. The future of backpacking. A scenario planning approach to the backpacker's travel behaviour. European Tourism Futures Institute. European Tourism Futures Report 7. URL: http://toerismenoordnederland.nl/wp-content/uploads/The-Future-of-Backpacking.pdf. Accessed: 12 April 2015

Wallop, H. 31 Jul 2014. Gen Z, Gen Y, baby boomers – a guide to the generations. URL: http://www.telegraph.co.uk/news/features/11002767/Gen-Z-Gen-Y-baby-boomers-a-guide-to-the-generations.html. Accessed: 12 April 2015

WYSE Travel Confederation. 25 Feb 2014a.10 things you might not know about the youth travel market. URL: http://www.wysetc.org/2014/02/25/10-things-you-might-not-know-about-the-youth-travel-market. Accessed: 6 April 2015

WYSE Travel Confederation. 11 Nov 2014b. Youth travel industry following global tourism growth trend and exceeding forecasts for 2014. URL: http://www.wysetc.org/2014/11/11/youth-travel-industry-following-global-tourism-growth-trend-and-exceeding-forecasts-for-2014. Accessed: 12 April 2015

Yeoman I., Hsu C.H.C., Smith K.A. & Watson, S. 2011. Tourism and demography. Good-fellow Publishers Ltd. Oxford

Appendices

Appendix 1. The survey

The Awareness and Concern of Information Security Risks Amongst Young Travellers

Hey there young traveller aged 18-32!

I am a hospitality management student in HAAGA-HELIA University of Applied Sciences and work at F-Secure, an online security and privacy company from Finland. For my thesis I decided to look into the privacy issues we face as young travellers, feeling forever compelled to be connected through our mobile devices. The idea is to find out how awareness of the information security risks that come along with these mobile devices affects our travel behavior.

The thesis is commissioned by F-Secure and therefore the results of this survey will be presented to them to hopefully help with future product developments aimed at travellers. All responses will remain entirely anonymous throughout the process and the final thesis can be found on Theseus.fi by June 2015.

If you have any questions concerning the survey or my thesis, please do not hesitate to contact me.
Thank you for your time!

Sincerely,
Kaisu Mäkelä

kaisu-linnea.makela@myy.haaga-helia.fi

1. How old are you? *

18

2. Gender *

Male Female

3. What is your nationality? *

Finnish Other, which?

Next -->

(1 of 7 pages)

4. Approximately how many times per year do you travel abroad?

0 1-2 3-5 over 5

5. Which of the following devices do you usually carry along with you when you travel?

Smartphone Touchscreen tablet Laptop None

<-- Previous Next -->

(2 of 7 pages)

6. Which of the following activities do you use your mobile device(s) for when travelling?

- [ ] Online social networks (e.g. Facebook, Twitter, Instagram, MySpace, etc.)
- [ ] Communication apps (e.g. WhatsApp, Skype, Facebook Messenger, SnapChat, etc.)
- [ ] Travel apps (e.g. TripAdvisor, eBooker, Airbnb, TripIt, etc.)
- [ ] Surfing the net
- [ ] Email
- [ ] Buying goods or services online
- [ ] Online banking
- [ ] Navigation (GPS)
- [ ] Taking pictures
- [ ] Storing usernames and passwords
- [ ] Keeping copies of passport/travel documents

<-- Previous Next -->

(3 of 7 pages)

7. How well informed do you feel about information security risks?

- ○ 1 - Not at all informed
- ○ 2 - Not very well informed
- ○ 3 - Fairly well informed
- ○ 4 - Very well informed

<-- Previous Next -->

(4 of 7 pages)

8. How concerned are you about the following risks regarding information security?

	0 - I haven't thought about it	1 - Not at all concerned	2 - Not very concerned	3 - Somewhat concerned	4 - Very concerned
a. Losing your device	○	○	○	○	○
b. Misuse of personal data (for sales and marketing purposes)	○	○	○	○	○
c. Not being able to access online services (e.g. banking services)	○	○	○	○	○
d. Your social media or email account being hacked	○	○	○	○	○
e. Identity theft (somebody stealing your personal data and impersonating you)	○	○	○	○	○
f. Being a victim of bank card or online banking fraud	○	○	○	○	○
g. Discovering malicious software (viruses etc.) on your device	○	○	○	○	○
h. Being tracked	○	○	○	○	○

<-- Previous Next -->

(5 of 7 pages)

9. Which of the following privacy measures have you taken to secure data on your mobile devices when travelling?

- [ ] You use a passcode to restrict access to your device
- [ ] You have antivirus software installed on your device
- [ ] You use a VPN whenever connected to a public WiFi
- [ ] You avoid connecting to public WiFis when travelling
- [ ] You remove/backup/encrypt files on your device before travelling - which?
- [ ] You make sure all apps and software are updated before travelling
- [ ] You have changed passwords to any accounts you may have used abroad after returning to your country
- [ ] Other, which?

<-- Previous Next -->

(6 of 7 pages)

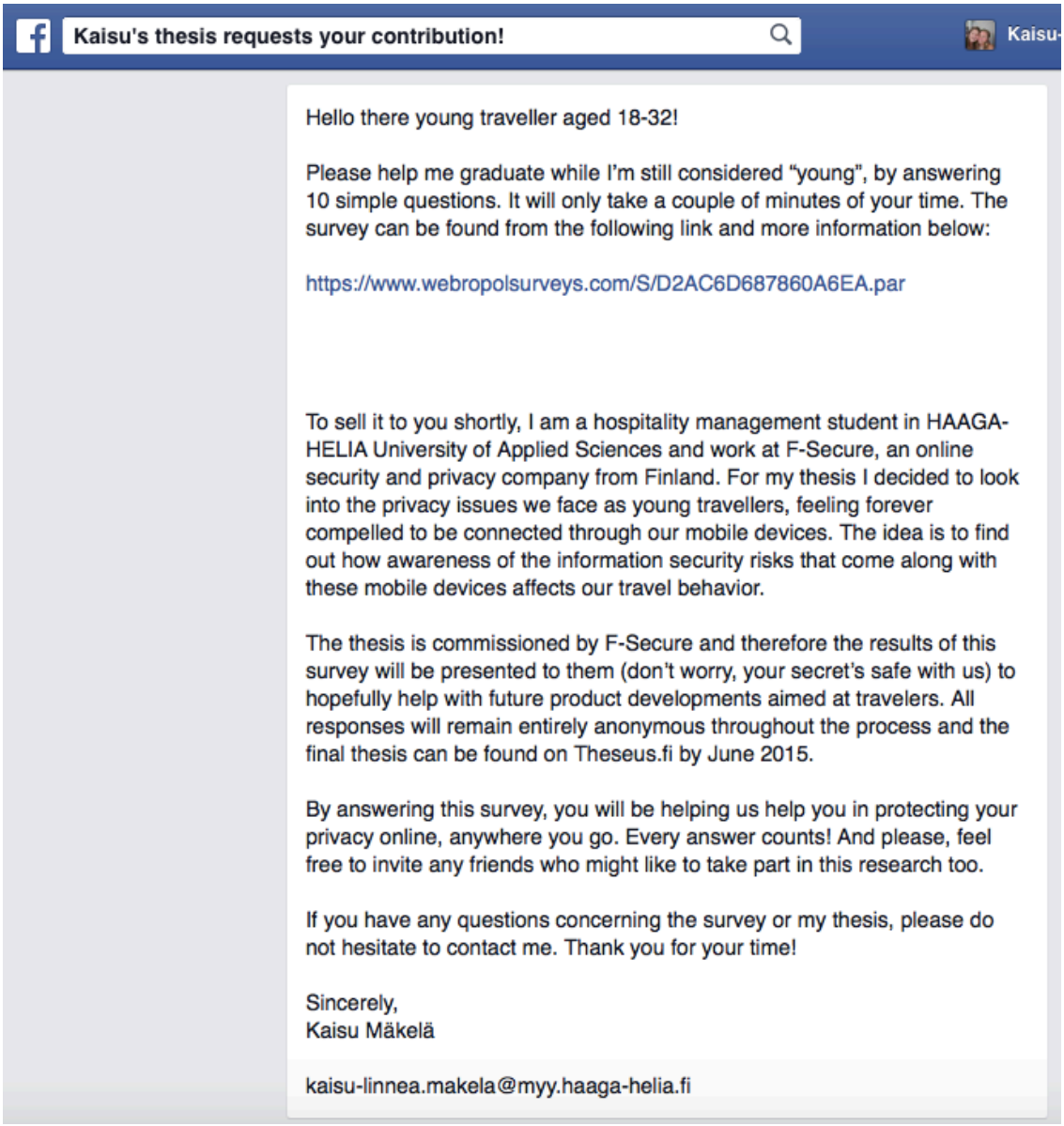
10. Do you have any personal experiences regarding personal data loss? Have you lost a phone or have any of your accounts been hacked? Please share your experience!

<-- Previous Submit

(7 of 7 pages)

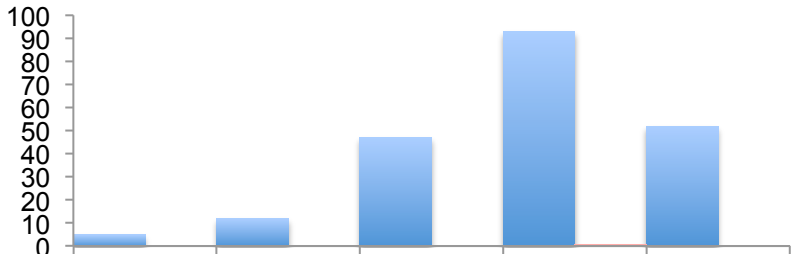
Thank you for your participation!

Appendix 2. The cover letter



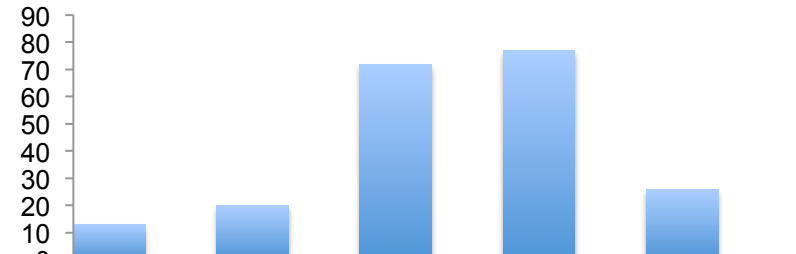
Appendix 3. Tables of levels of concern per threat (survey question 8)

Losing your device



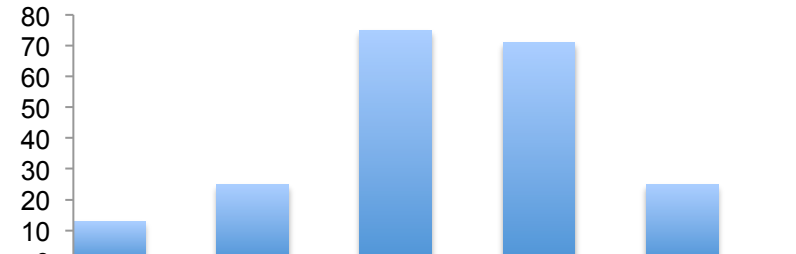
	0 - I haven't thought about it	1 - Not at all concerned	2 - Not very concerned	3 - Somewhat concerned	4 - Very concerned
N	5	12	47	93	52
Percentage	2.39%	5.74%	22.49%	44.50%	24.88%

Misuse of personal data



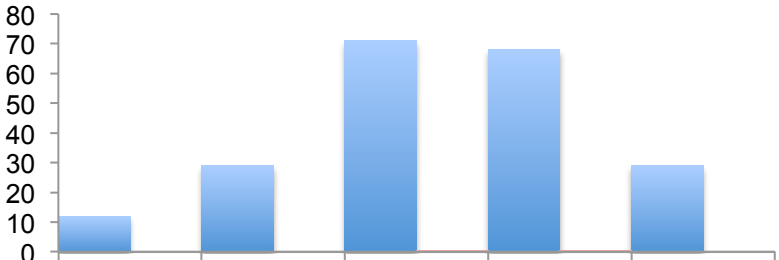
	0 - I haven't thought about it	1 - Not at all concerned	2 - Not very concerned	3 - Somewhat concerned	4 - Very concerned
N	13	20	72	77	26
Percentage	6.25%	9.62%	34.62%	37.02%	12.50%

Not being able to access online services



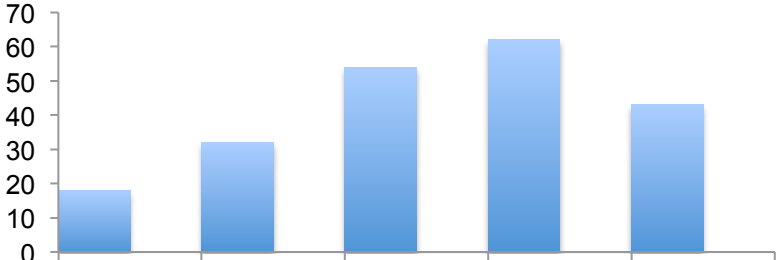
	0 - I haven't thought about it	1 - Not at all concerned	2 - Not very concerned	3 - Somewhat concerned	4 - Very concerned
N	13	25	75	71	25
Percentage	6.22%	11.96%	35.89%	33.97%	11.96%

Social media or email account being hacked



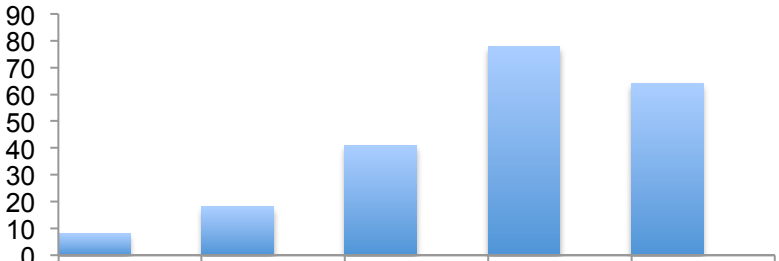
	0 - I haven't thought about it	1 - Not at all concerned	2 - Not very concerned	3 - Somewhat concerned	4 - Very concerned
N	12	29	71	68	29
Percentage	5.74%	13.88%	33.97%	32.54%	13.88%

Identity theft

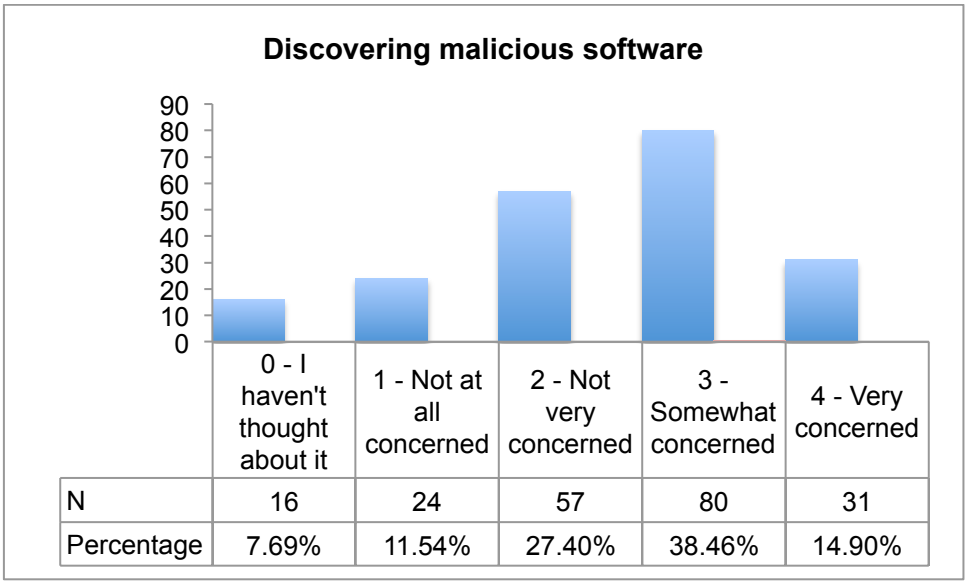


	0 - I haven't thought about it	1 - Not at all concerned	2 - Not very concerned	3 - Somewhat concerned	4 - Very concerned
N	18	32	54	62	43
Percentage	8.61%	15.31%	25.84%	29.67%	20.57%

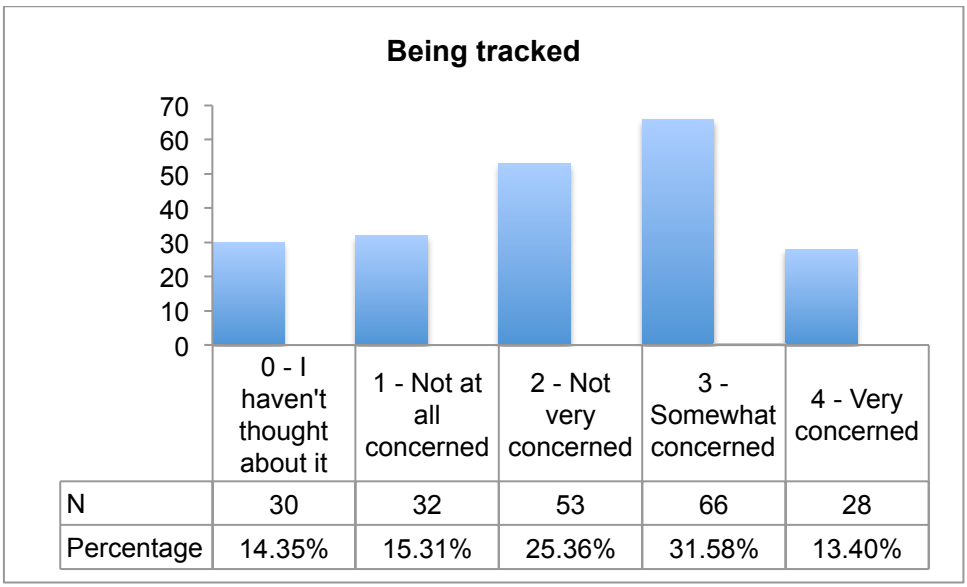
Victim of bank card or online banking fraud



	0 - I haven't thought about it	1 - Not at all concerned	2 - Not very concerned	3 - Somewhat concerned	4 - Very concerned
N	8	18	41	78	64
Percentage	3.83%	8.61%	19.62%	37.32%	30.62%



	0 - I haven't thought about it	1 - Not at all concerned	2 - Not very concerned	3 - Somewhat concerned	4 - Very concerned
N	16	24	57	80	31
Percentage	7.69%	11.54%	27.40%	38.46%	14.90%



	0 - I haven't thought about it	1 - Not at all concerned	2 - Not very concerned	3 - Somewhat concerned	4 - Very concerned
N	30	32	53	66	28
Percentage	14.35%	15.31%	25.36%	31.58%	13.40%

Appendix 4. Open-ended responses to survey question 10

- None. Have been lucky so far.
- My phone was stolen once and I felt quite exposed. I lost all my contacts and pictures. And I immediately changed my email and social networking account passwords. I didn't go to the police as it is impossible to find a phone after it's stolen, and police do not actively search for it. Nowadays, I copy or move photos and contacts to another location when my phone gets full. I also delete photos I have moved from my phone.
- Never happened to me
- no experience
- My smartphone got stolen a couple of years ago in Spain. I immediately called my brother in Finland and he changed all my passwords (to gmail, facebook...). It scared me how easy it actually is to use someone others phone with only breaking the pincode/screencode. After that you can access everything without passwords.
- I have no such experiences
- Nothing have happened..at least not yet... ;)
- Sorry, no experiences.
- Phone stolen along with ID and debit card (in Finland). Thieves got access to personal information including finding out my home address. They managed to call paid sex lines etc before I cancelled the line and I had to pay the 300+ euro bill (insurance wouldn't cover). Phone was not a smartphone. Perhaps a phone with a lock screen could've prevented this.

  They also used my personal information to order large, expensive things online for home delivery as a prank. These included a buggy and gym equipment which thankfully weren't paid for. I had to cancel anything else they might be able to abuse with access to all my personal info, such as library cards etc.
- Thank god no :D
- Once my phone got stolen when I was travelling.
- Somebody hacked my pc once and use my IP to open fake account on eBay.
- No I haven't.
- None of these things have happened to me. I consider myself very lucky!
- none
- No phones lost, but once I received a warning from my Outlook email account that it was trying to be reached from Ukraine. They suggested I change my password, which I did nad everythin seemed/seems to be fine after that.
- No but my friend's phone was stolen a few weeks ago on a holiday in bali.The thiefs took her bag with all her personal stuff during a ride with scooters.
- No.
- Had phone stolen, although it was password secured and had no important info on, so luckily no bad consequences
- Nope, sorry.

- I think my twitter account has been hacked once.
- None, everything has been safe!
- Luckily no.
- I think my e-mail account was once hacked because I received a warning about it. I immediately changed my password and the problem never occurred again.
- I have (luckily) no personal experience regarding personal data loss.
- I haven't really had any experiences with personal data loss. I'd like to think it's because I'm carefull with my phone where ever I go. I'm always aware of where I have my phone, have everything behing a password (ofcourse with capital letters, small letters, numbers and special symbols) that only I know. I don't know wether I'm fooling myself or not about the security of my personal data, but I've travelled a lot, and never had any problems with it.
- None
- Luckily, no.
- On my last trip abroad, my main email account was hacked and someone changed my password. I had to create a new one and lost all my contacts.
- Nope.
- Credit card was copied while travelling in Netherlands (Amsterdam). Credit card has been tried to use.
- Nothing ever happened. Knocking wood.
- My phone had got stolen before and I'm worrying that the theft or whoever is using my phone can see my photo through iCloud. That's why now I logged out from iCloud and stop syncing my photos. It would be nice to know if there is a way out from this trouble though.
- none
- Someone stole my phone and I used to have all my nip's of my credit and debit card in some notes. So I have to called the bank and ask for call in every charge I made.
- Fortunately, not yet.
- Luckily my e-mail and social media accounts haven't been hacked, at least not yet, so I have no experience in how dealing in these situations. I prefer not saving passcodes to those accounts when entering from my smartphone so to minimize the risks of beeing hacked in case of losing the phone.
- No, I have not lost any data or any items, but I'm trying to be careful when and where I use my devices. Carry the absolute minimum, and protect them with good passwords.
- Never lost any data. Automatic backups to my own personal cloud server (running in 2 different locations) from every devices thru vpn. Backup is end to end encrypted.
- No.....
- No
- I have no smartphone.
- Tengo varios correos (gmail, hotmail, universidad...), cuentas en Apple, Windows, diferentes aplicaciones, juegos... y como cada contraseña pide una cosa (numeros, capital letters, 6-8 caracteres...) muchas veces no me acuerdo de las diferentes contraseñas que tengo :D :D

(Translation: *I have various emails (gmail, hotmail, university…), accounts for Apple, Windows, different applications, games.. and as each password requires something (numbers, capital letters, 6-8 characters…) I often don't remember the different passwords I have :D :D*)

- I've broken a phone (water damage - dropped it in the sink at an airbnb while washing dishes). Lost some photos, but nothing more important than that.
- I have also dropped the laptop so that the screen chipped and had to be replaced - that was the scare I needed to start backing up my stuff.
- No, never so far. I always use public wifi spots too.
- Nope
- I never haven´t lost my phone
- -
- noup
- No :)
- Luckily, no such experiences. Maybe that's why I don't use much precaution while travelling, yet. I haven't been hacked, that I know of.
- My laptop was hacked while I was in university using a public network. The hacker took one of my essays and handed it in to the prof as their own. Fortunatly, the hacker came clean and stated the essay wasn't hers. When I found out I had been hacked, I immediately researched ways to decrease any risks of being hacked... especially that I had plenty of personal data on my computer. Who knows what else was taken from me. All passwords have now been changed and my firewall and other security/privacy settings have been updated to the maximum security possible!
- No, I haven't.
- No
- No
- I have lost an iPad, left it to aeroplane, and haven't heard of it since. There was a security code in use. I changed all the passwords after noticing I have lost it, and contacted the flight company, but they did not find it. Probably some cleaner or other personnel of the aircraft has taken it and sold it. I always thought that no one could use my device, but obviously you can..
- My email account was hacked into when I was younger and the person who did it sent emails to my friends impersonating me. I also once had some sort of a virus that sent weird emails to everyone on my contact list.
- No experiences of such thing
- No.
- I have had my hotmail account hacked a few years ago and lost all my emails and communications from that account and needed to get a new email after